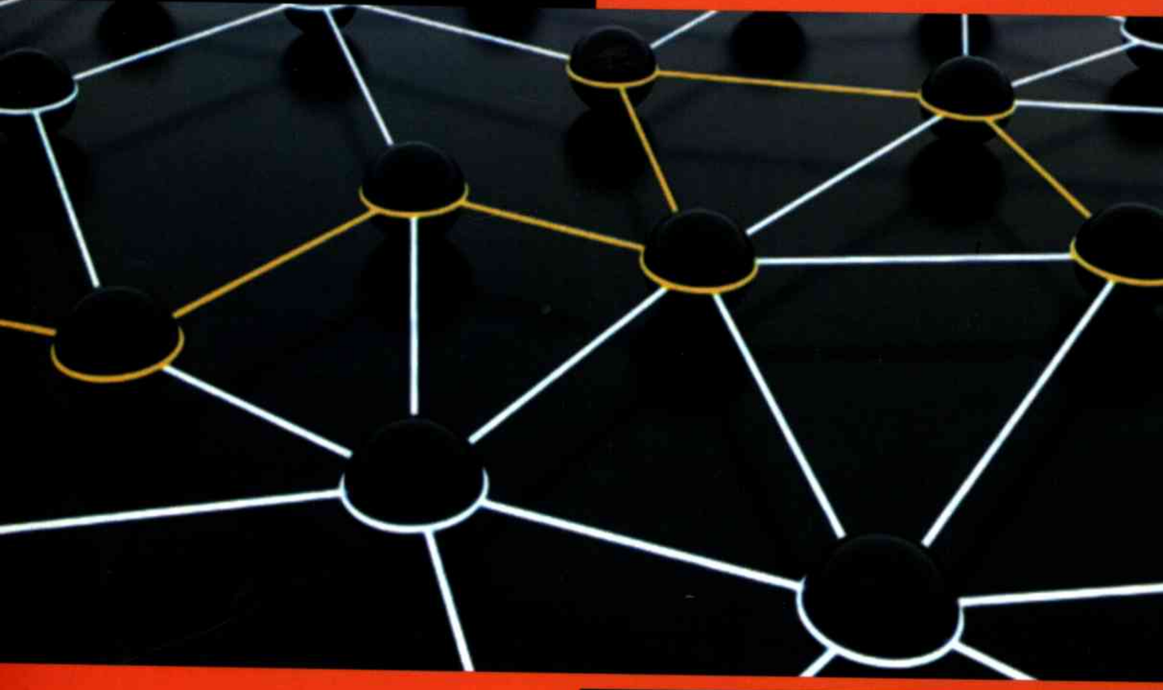
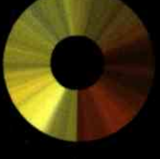
آموزش جامع شبکه



مؤلف : کاوه اجتهادی
(دارای گواهینامه بین المللی + Network)

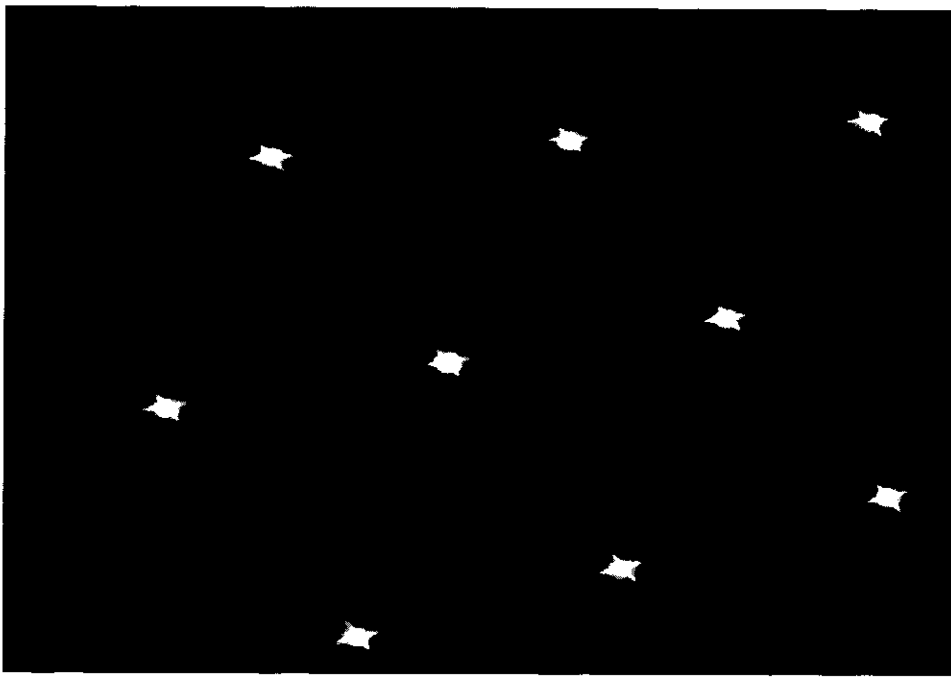
مطابق با سرفصل‌های آزمون
بین المللی - Network



مجموعه از آزمون‌های
شبیه سازی شده در دیسکت ضمیمه
این کتاب در دسترس شماست

بسم الله الرحمن الرحيم

آموزش جامع شبکه



بر اساس سرفصل های +Network

کاوه اجتهادی

سر شناسه	: اجتهادی، کاوه، ۱۳۵۹-
عنوان و نام پدیدآور	: آموزش جامع شبکه، / مؤلف کاوه اجتهادی
مشخصات نشر	: تهران؛ کاوه اجتهادی، ۱۳۸۹
مشخصات ظاهری	: ۲۹۲+۱۲ ص، مصور، جدول
شابک	: 6 - 5318 - 04 - 964 - 978 قیمت : ۷۹۰۰۰ ریال
وضعیت فهرست نویسی	: فیپا
موضوع	: شبکه‌های کامپیوتری-- راهنمای آموزشی
موضوع	: شبکه‌های کامپیوتری-- آزمون ها
رده بندی کنگره	: ۱۳۸۹ ۸ آ ۲۷ الف/ ۵/ TK ۵۱۰۵
رده بندی دیویی	: ۰۰۴/۶
شمارهٔ کتابشناسی ملی	: ۲۰۰۶۷۶۹

انتشارات ناقوس

www.naghoospress.ir

نام کتاب	:	آموزش جامع شبکه
ناشر	:	مؤلف
ناشر همکار	:	انتشارات ناقوس
مؤلف	:	کاوه اجتهادی
ویراستار	:	مهندس طاهره اجتهادی
ناظر چاپ	:	انتشارات ناقوس
نوبت چاپ	:	اول- ۱۳۸۹
شمارگان	:	۱۰۰۰ نسخه
شابک	:	۹۷۸-۹۶۴-۰۴-۵۳۱۸-۶
ISBN	:	978 - 964 - 04 - 5318 - 6
بها به همراه CD	:	۷۹۰۰۰ ریال

مرکز پخش تهران : ۴۴۲۷۰۱۴۸ - ۴۴۲۵۰۸۷۸ - ۰۹۳۶۳۷۸۲۶۸۸

WWW.FAVALEARN.COM

موضوعات کتاب در یک نگاه

فهرست مطالب

پیش گفتار

اگر شما در زمینه فناوری اطلاعات و ارتباطات مشغول فعالیت هستید یکی از مواردی که می تواند جایگاه شما را در شرکت یا سازمانی که در آن مشغول کار هستید ارتقا دهد اخذ گواهینامه های تخصصی است. برخی از این گواهینامه ها مربوط به داشتن تخصص در مورد محصولات یک شرکت خاص است برخی از این گواهینامه ها عبارتند از CCNA شرکت سیسکو، MCSE شرکت مایکروسافت و گواهینامه های سرور های HP .اما برخی دیگر مانند گواهینامه های موسسه CompTIA بر روی تکنولوژی تاکید داشته و وابسته به هیچ محصولی نیستند و از آن برای آموزش مبانی و مقدمات فناوری اطلاعات و ارتباطات استفاده می نمایند. البته ذکر این نکته ضروری است که در تمامی این گواهینامه ها داشتن گواهینامه +Netwwork به عنوان یک پیش نیاز معرفی شده و در مباحث ابتدایی آنها مطالب این کتاب به صورت خلاصه آمده است.

این گواهینامه ها اگر از سوی شرکت های معتبر صادر شود نشان دهنده دانش فنی و تجربه فرد است که در تمامی شرکت ها دارای اعتبار می باشد.

در این کتاب سعی نمودم که برای شما تمامی موارد لازم جهت شرکت در آزمون و قبولی در آن را گرد هم آورم. برای این کار از تجربه شخصی برای شرکت در آزمون استفاده نمودم و مطالبی را به نسخه اصلی کتاب اضافه نمودم که می تواند کمک شایانی برای موفقیت به شما انجام دهد.

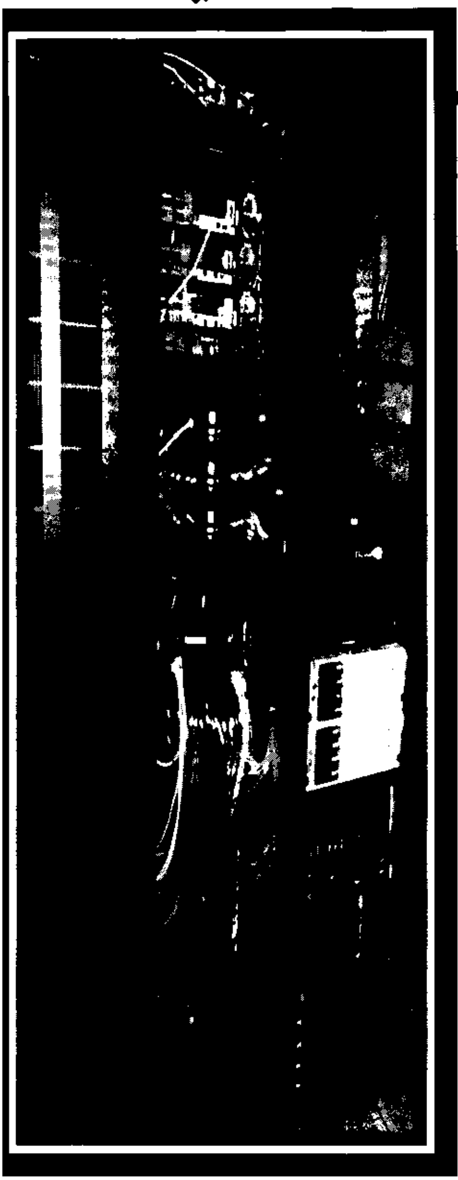
گواهینامه +Network چیست ؟

+Network گواهینامه ای است که توسط موسسه CompTIA تهیه شده است.هدف اصلی این موسسه تهیه منابع استاندارد برای کارشناسان و علاقمندان به فناوری اطلاعات می باشد. برای سنجش توان علمی و فنی علاقمندان هم آزمون هایی در سراسر دنیا برگزار می نماید که این گواهینامه ها توسط شرکت های معتبر به رسمیت شناخته می شود. برخی از این شرکت ها عبارتند از:

- IBM
- Compaq
- Microsoft
- UsRobotics
- Novell

مقدمه و پیش گفتار

پیش گفتار



در این بخش با مقدمات آزمون و نحوه شرکت در آن صحبت خواهیم نمود.

مقدمه و پیش گفتار

در این آزمون مطالب متنوعی مانند توپولوژی های شبکه ، مدل OSI و تجهیزات شبکه مورد بحث قرار می گیرد.علاوه بر آن نحوه برخورد با مشکلات و رفع آنها که شاید مهمترین وظیفه یک مدیر شبکه است هم بررسی می شود.

چرا اخذ این گواهینامه مهم است؟

این آزمون ، جدید و به روز است و هر چند سال یکبار ارتقا یافته و به روز می شود تا از تکنولوژی های جدید هم پشتیبانی نماید. از آنجا که این آزمون به شرکتی خاص و یا محصولات خاصی بستگی ندارد و همینطور توسط موسسه ای معتبر مانند CompTIA برگزار می شود می تواند توان علمی و فنی فرد را تایید نماید. با این گواهینامه شما می توانید جایگاه علمی خود را افزایش داده و اطلاعات خود را به روز نگاه دارید.

مطالعه این کتاب به چه کسانی توصیه می گردد؟

اگر شما یکی از هزاران علاقمند به شرکت در آزمون +Network هستید و تصمیم به شرکت در آزمون دارید درنگ نکنید. زیرا این کتاب بر مبنای سرفصل های مصوب شرکت CompTIA تهیه شده است.

آزمون +Network برای سنجش تجربه و دانش فنی افراد تهیه شده است و هر کارشناس با حد اقل ۲ سال کار در زمینه شبکه و مطالعه این کتاب می تواند در این آزمون موفق شود.

علاوه بر این موارد این کتاب می تواند مرجعی کامل برای آموزش شبکه در دوره های آزاد و دانشگاهی باشد.

چگونه شما می توانید در این آزمون شرکت کنید؟

شرکت در این آزمون برای همه علاقمندان آزاد است و نیاز به هیچ پیش نیازی ندارد.این آزمون توسط شرکت معتبر Thompson Prometric و یا Pearson VUE که تمامی آزمون های تخصصی را برگزار می کنند اجرا می شود که این نشان از ارزش و اعتبار این آزمون دارد. این آزمون ها در دفاتر رسمی این شرکت ها در سراسر دنیا انجام می گیرد و هزینه آن در سراسر دنیا یکسان است که هزینه آزمون را می توان از وب سایت شرکت کامپتیا به آدرس www.comptia.org مشاهده نمود.

مشخصات آزمون

مطالب این بخش مربوط به سال ۲۰۱۰ میلادی بوده و به نقل از وب سایت موسسه کامپتیا می باشد.

تعداد سوالات آزمون :

تعداد سوالات ۱۰۰ سوال تستی است .برخی از تست ها حالت خاص دارند و بیش از یک پاسخ صحیح دارند که باید تمامی پاسخ های صحیح انتخاب شود. در صورت انتخاب بخشی از سوالات هم پاسخ نادرست محاسبه می شود.این آزمون نمره منفی ندارد.

زمان پاسخگویی :

زمان پاسخگویی ۹۰ دقیقه است که توسط سیستم محاسبه می گردد و پس از اتمام آن دسترسی شما به سوالات قطع می شود.پس از شروع زمان آزمون متوقف نمی شود.

حد نساب قبولی :

کسب امتیاز ۷۲۰ از ۹۰۰ امتیاز ممکن برای اخذ گواهینامه لازم است.در این آزمون ارزش همه سوالات یکسان نیست.

پیش نیاز های پیشنهادی :

- گذراندن دوره و یا اخذ گواهینامه CompTIA A+ به همراه ۹ ماه تجربه شبکه
- تنها ۲ سال تجربه در شبکه

زبان های آزمون :

این آزمون به زبان های انگلیسی ، آلمانی و اسپانیایی برگزار می شود. در زمان ثبت نام شما یکی از این زبان ها را انتخاب می نماییدو در زمان برگزاری آزمون با همان زبان انجام خواهد شد.

کد آزمون :

این آزمون با کد N10-004 در سراسر دنیا برگزار می شود. این نسخه از آزمون از سال ۲۰۰۹ شروع شده است . و حداقل تاپایان سال ۲۰۱۰ ادامه خواهد داشت.

درباره نویسنده

من نویسنده کتاب کاوه اجتهادی دارای مدارک تخصصی CCNA، CWNA ،Network+، A+ هستم که بالغ بر ۱۰ سال تجربه در شاخه های مختلف فناوری اطلاعات و ارتباطات دارم. سعی کردم با تالیف این کتاب تجربه

مقدمه و پیش گفتار

خود را در اختیار دیگران هم قرار دهم . شبکه همانند دیگر علوم فناوری اطلاعات و ارتباطات هر روزه پیشرفت نموده و محصولات و تکنولوژی های جدیدی معرفی می شوند. یکی از نیاز های مهم به روز بودن معلومات و دانش هر مدیر شبکه است. این کار با مطالعه منابع جدید امکانپذیر می گردد اما دسترسی به این منابع برای همه به آسانی صورت نمی گیرد.به دلیل تحریم هایی که در طول چند سال اخیر علیه ایران انجام شد کارکمی سخت تر گردید.مشکل اصلی برای کاربران ایرانی زبان منابع علمی است. متاسفانه امروزه زبان علم انگلیسی است حال آنکه در گذشته زبان علم فارسی و عربی بوده است.

در زمان آمادگی برای شرکت در آزمون های تخصصی یکی از مواردی که همیشه من را آزار می داد نبودن منابع مناسب بود منابعی به روز و قابل اعتماد در عین حال با قیمت مناسب . از همان زمان تصمیم گرفتم که منابع مورد نظر هم وطنان و هم زبانان عزیز را با زبان فارسی فراهم نمایم.این کار را با این کتاب آغاز نمودم و ان شاءالله با منابع دیگر شبکه ادامه خواهم داد.

در پایان از زحمات تمامی اساتید بزرگواری که برای رسیدن به این جایگاه مرا یاری نمودند صمیمانه تشکر می نمایم.

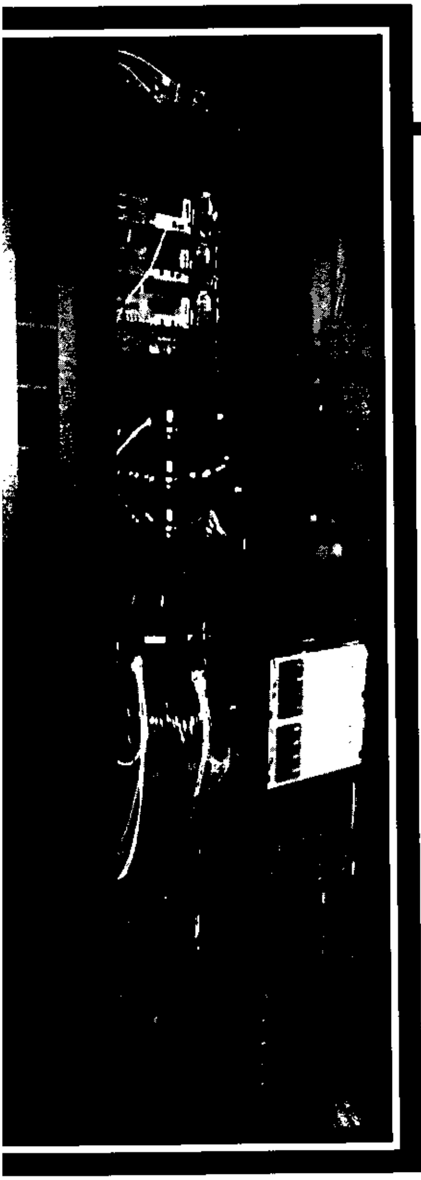
پست الکترونیکی : netplus.ir@gmail.com آماده دریافت نظرات ؛پیشنهادات و انتقادات خوانندکان و کارشناسان محترم می باشد.به روز رسانی و پاسخ به سوالات و مشکلات از طریق وب سایت www.favalean.com هم امکانپذیر است.

کاوه اجتهادی

فروردین ۱۳۸۹

فصل اوّل

مبانی شبکه



شما در این فصل با این مفاهیم آشنا خواهید شد:

۱-۱ آشنایی با توپولوژی های فیزیکی ومنطقی شبکه و آشنایی با نقاط ضعف و قوت هر کدام

- ستاره ای
- خطی
- شبکه ای
- دایره ای

۱-۲ شناخت تکنولوژی های 802.2 ، 802.3، 802.5، 802.11،

FDDI و آشنایی با مولفه هایی مانند:

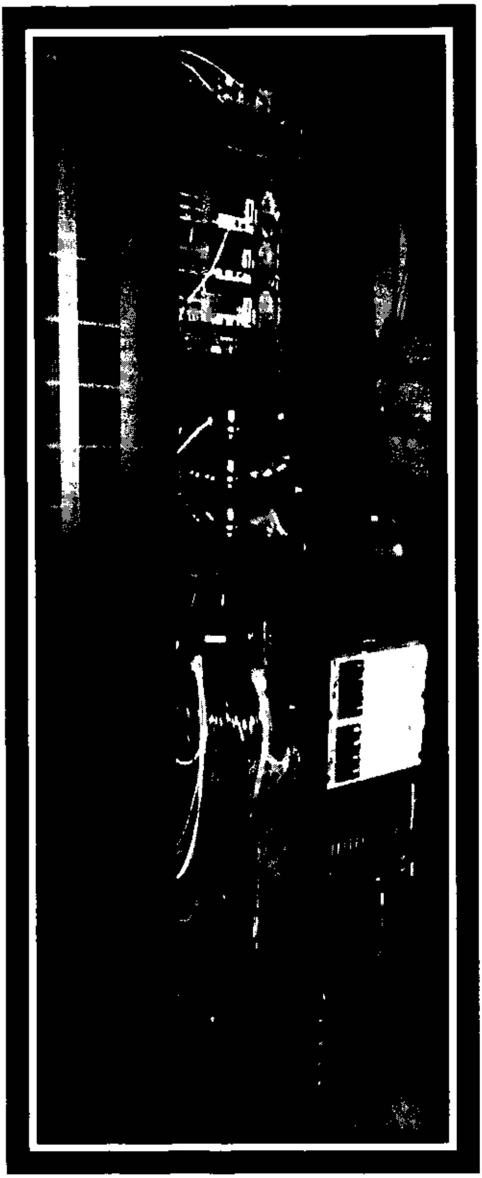
- سرعت
- CSMA/CA
- CSMA/CD
- توپولوژی
- ساختار فیزیکی

۱-۳ بررسی مولفه های فیزیکی مانند: سرعت،طول،توپولوژی و نوع کابل در استاندارد های زیر:

- 10Base-FL،10Base-T
- 100Base-FX،100Base-TX
- 1000Base-SX،1000Base-CX ،1000Base-TX

  1000Base-LX

- 10GBase-SR 10GBase-LR 10GBase-ER



۱-۴ آشنایی با اتصالات کابل ها و نحوه استفاده از آنها

- Rj-11
- Rj-45
- F-type
- ST
- SC
- IEEE1394
- LC
- MTRJ
- USB

۱-۵ آشنایی با استاندارد کابل های ارتباطی و مشخصات آنها

- Category 3,5,5e and 6
- UTP
- STP
- Coaxial
- SMF
- MMF

۱-۶ آشنایی با عملکرد تجهیزات شبکه

- Hub
- Switch
- Bridges
- Routers
- Gateway
- CSU/DSU
- NIC
- ISDN
- WAP
- Modem
- Transceiver
- Firewall

۱-۷ شناخت حداقل های لازم جهت اتصال یک کاربر یا یک ایستگاه کاری به شبکه واستفاده از منابع اشتراکی آن

شبکه چیست؟

در دنیای کامپیوتر به ۲ یا چند سیستم متصل به هم شبکه یا Network میگویند. که می توانند یک سری منابع را به اشتراک گذارند.

این منابع می تواننداده ها؛ چاپگر یا دسترسی به اینترنت و یا تلفیقی از این ها باشد.

در ادامه به بررسی تفصیلی شبکه از لحاظ محدوده عملکرد ،نوع ارتباط ، و ساختار فیزیکی آنها می پردازیم.

انواع شبکه از نظر نوع ارتباط

شبکه ها از نظر نوع ارتباط به ۲ شاخه اصلی تقسیم می شوند:

- شبکه های سیمیWired
- شبکه های بدون سیم Wireless

شبکه های سیمی (Wired Networks):این شبکه ها جهت ارتباط از سیم استفاده می کنند.ممکن است این کابل کواکسیال ؛UTP یا فیبر نوری باشد.

شبکه های بیسیم (Wireless Networks) :که جهت ارتباط در محدوده ای معین و با شرایط و ظوابطی خاص بدون بکار بردن سیم استفاده میشود.

در مورد انواع استاندارد ها و دیگر مشخصات این شبکه ها در مباحث آینده به تفصیل خواهیم پرداخت.

انواع شبکه از نظر محدوده عملکرد

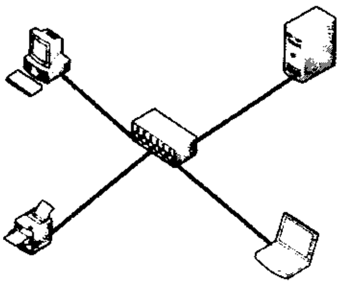
شبکه ها از نظر محدوده عملکرد به طور کلی به ۴ نوع تقسیم می شوند.

- شبکه های محلی LAN
- شبکه های شهری MAN
- شبکه های گسترده WAN
- شبکه های شخصی PAN

شبکه های بدون سیم (Wireless Networks) نیز از این قاعده کلی تبعیت می کنند.لازم به ذکر است در شبکه های بدون سیم نوع دیگری با نام WPAN (Personal Area Network)هم وجود دارد که به نام شبکه های شخصی مشهور است و معمولا با تکنولوژی Blue Tooth در مقیاس بسیار کوچک ایجاد می شود.

شبکه محلی LAN (Local Area Network)

شبکه های محلی یا همان LAN شبکه ای است در مقیاس جغرافیایی کوچک که تعداد محدودی سیستم را به هم متصل می نماید. معمولا محدوده این نوع شبکه در داخل یک ساختمان می باشد.

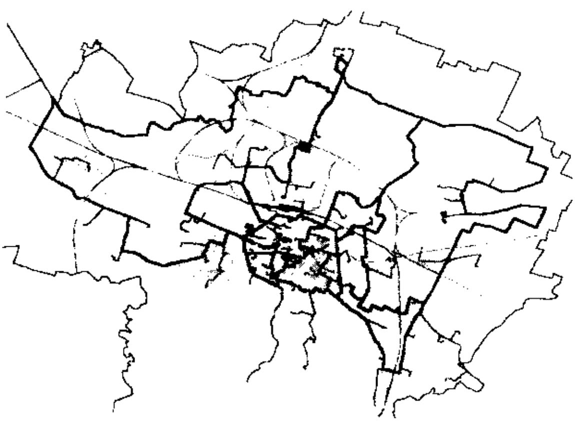


این شبکه می تواند به دلایل زیادی ایجاد گردد از جمله :

- به اشتراک قرار دادن فایل ها
- به اشتراک قرار دادن چاپگر
- ارسال و دریافت داده ها بین سیستم های شبکه
- انجام بازی های رایانه ای چند نفره

معمولا سرعت ارتباط و انتقال داده ها در این نوع شبکه بسیار بالا می باشد.البته فاکتور های مهم دیگری نیزدر هرشبکه وجود دارد مانند نوع وسیستم ارتباط وساختار شبکه که در بخش های بعدی به آن می پردازیم.

شبکه شهری MAN(Metropolitan Area Network)



شبکه های شهری یا همان MAN شبکه ای است در مقیاس جغرافیایی متوسط که بین ۵ تا ۵۰ کیلومتر وسعت دارد که تعداد محدودی سیستم را به هم متصل می نماید. این شبکه می تواند ارتباطی بین اجزا یک سازمان را تامین نموده و یا ارتباطی عمومی باشد. در این گونه ارتباطات با توجه به وسعت محدوده از زیر ساخت های فیبر نوری کمک گرفته می شود و یا همچنین می توان از شبکه های بدون سیم و تکنولوژی های جدید این شاخه مانند Wi-MAX هم استفاده نمود.

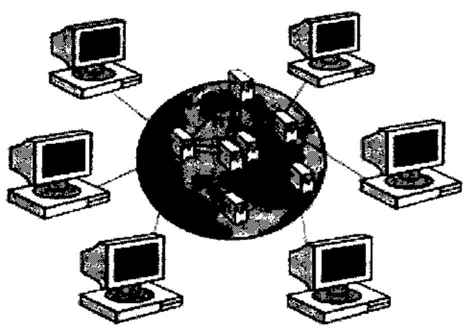
سرعت و میزان ارسال و دریافت داده ها به عوامل مختلفی از جمله ساختار و تکنولوژی ارتباطی بین اجزا مرتبط می باشد.

شبکه گسترده(WAN (Wide Area Network

شبکه های گسترده یا همان WAN شبکه ای است در مقیاس جغرافیایی وسیع که معمولا بیشتر از ۵۰ کیلومتر وسعت دارد که از به هم پیوستن تعدادی شبکه محلی به هم بوجود می آید.البته این تعریف استثناء هم دارد.

در مورد شبکه اینترنت که نمونه ای از این ساختار است،اتصال دو کامپیوتر در دو قاره مختلف نمونه ای از این ساختار شبکه است.و نیازی به اتصال دو یا چند شبکه محلی نیست.

سرعت و میزان ارسال و دریافت داده ها به عوامل مختلفی از جمله ساختار و تکنولوژی ارتباطی بین اجزا مرتبط می باشد.



انواع شبکه از نظر ارتباط

شبکه ها از نظر ارتباط به طور کلی به ۲ بخش تقسیم می شوند :

- Peer-To-Peer ارتباط یک به یک
- Client –Server ارتباط سرور و کاربر

در شبکه های Peer-To-Peer کامپیوتر ها فاقد یک سیستم اتصال مرکزی (Central Unit)هستند وهر سیستم دارای فضای ذخیره و بازیابی اطلاعات مربوط به خود است.

در شبکه های Client –Server یک سیستم عامل شبکه موجود است که وظیفه مدیریت شبکه را از نقطه مرکزی به عهده دارد که همان Server است. تمامی سیستم ها درخواست ها و اطلاعات مورد نیاز خود را به سیستم مرکزی می فرستند.

در این بخش به شناخت ۳ مفهوم ضروری در شبکه خواهیم پرداخت:

- ایستگاه کاری (Workstation)
- میزبان (Host)
- سرویس دهنده (Server)

ایستگاه کاری (Workstation)

ایستگاه کاری یا همان Workstation سیستمی است که از لحاظ کیفیت قطعات و کارآیی سیستم نسبت به رایانه های شخصی بالاتر است. این سیستم ها نیز برای استفاده یک کاربر طراحی شده اند. به بیان دیگرایستگاه کاری می تواند یک کامپیوتر با قدرت پردازش بالا و گرافیک قوی باشد که بتواند از عهده چندین کار با هم برآید.

میزبان (Host)

میزبان یا همان Host در واقع به هر دستگاهی که به شبکه متصل می شود اطلاق می گردد. به بیان دیگر تفاوت یک ایستگاه کاری و یک میزبان در این است که ایستگاه کاری حتماً می بایست کامپیوتر باشد در حالی که میزبان می تواند چاپگر و یا هر وسیله دیگر متصل به شبکه باشد.

در سیستم های مبتنی بر پروتکل TCP/IP به هر وسیله ای که دارای حداقل یک آدرس IP باشد میزبان یا کاربر می گویند.

سرویس دهنده (Server)

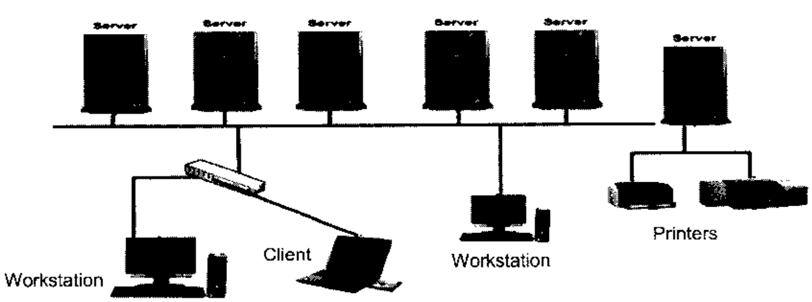
سرویس دهنده یاServer ارایه دهنده سرویسی در شبکه می باشد.بطور معمول سرورها کامپیوتر های بسیار قدرتمندی هستند که دارای نرم افزاری خاص برای مدیریت و سرویس دهی به شبکه می باشند که به "سیستم عامل شبکه" مشهور هستند.

سرور ها معمولاًبرای اجرای یک هدف در نظر گرفته می شوند.البته این بدان معنی نیست که سرورها نمی توانند چندین کار را باهم انجام دهند،بلکه به این دلیل است که برای بالا بردن کیفیت و کارآیی سرور ،آنها برای انجام کار خاصی منحصر می شوند.

در این قسمت با برخی انواع سرور و عملکرد آنها آشنا می شویم:

- سرور فایل ها (File Server):این سرور برای نگهداری و پخش فایل ها در شبکه بکار می رود.
- سرور چاپگر (Print Server):کنترل و نظارت بر عملکرد یک یا چند چاپگر درون شبکه از وظایف این سرور است.
- سرور پروکسی(Proxy Server):مفهوم پروکسی یعنی به نمایندگی از طرف دیگر اعضا می باشد که در واقع نقش واسط را بین داخل و خارج شبکه دارد.هدف از ایجاد این سرویس می توان بالا بردن امنیت شبکه،اعمال برخی محدودیت ها و یا حفظ هویت کاربران شبکه باشد.
- سرور پست الکترونیکی(Electronic Mail server):این سرور وظیفه دریافت و ارسال نامه های الکترونیکی کاربران شبکه را به عهده دارد ومعادل سرویس پست می باشد.
- سرور دسترسی راه دور(Remote Access Server):در واقع این سرویس جهت اتصال کاربران خارج از شبکه به منابع داخل شبکه بکار می رود.این اتصال ممکن است از طریق مودم و یا از طریق پروتکل IP انجام گیرد.
- سرور وب (WEB Server): نگهداری و ارسال صفحات وب برای کاربران شبکه از طریق پروتکل HTTP (Hyper Text Transfer Protocol) بر عهده این سرور می باشد.
- سرویس دهنده تلفن(Telephony Server):این سرور همانند یک دستگاه پاسخگویی تلفنی هوشمند عمل نموده و وظیفه مسیر یابی ،اتصال و یا ضبط مکالمات تلفنی را به عهده دارد.

شمای یک شبکه فرضی به شکل زیر است:



البته لازم به ذکر است که دسترسی فیزیکی به شبکه می بایست کنترل شده بوده و تابع قرارداد های امنیتی شبکه باشد تا شبکه دچار اشکال و اختلال نگردد.

تقسیم بندی شبکه از نظر نحوه ارتباط:

هماتگونه که شما در این فصل آموختید هدف اصلی شبکه به اشتراک قرار دادن منابع است.چگونگی انجام این کار بستگی به ساختار شبکه و سیستم عامل شبکه داردکه ازنظرنوع ارتباط به ۲ بخش تقسیم می شوند :

- Peer-To-Peer Networks
- Client –Server Networks

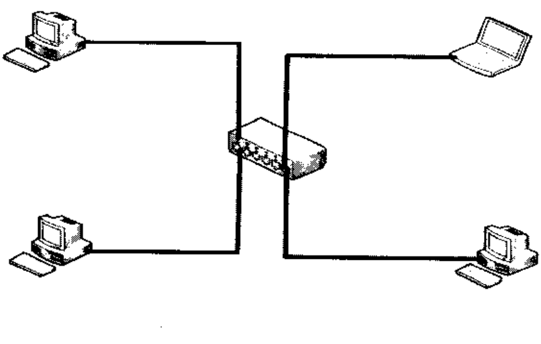
هرگاه شما از بیرون به یک شبکه محلی بنگرید در نگاه اول نوع آن را نمی توانید تشخیص دهید.می بایست یک نوار ویدئویی از نوع عملکرد یک روز این شبکه تهیه و در اختیار شما قرارگیرد تا با بررسی نوع عملکرد به شواهدی دست پیدا کنید.

شما از طریق بعضی سرنخ ها می توانید به نتیجه برسید اما نتیجه قطعی نیازمند شناخت دقیق هرکدام از این شبکه ها می باشد. در این بخش به بررسی هرکدام از این شبکه ها می پردازیم.

شبکه های Peer-To-Peer

در شبکه های یک به یک کامپیوتر ها فاقد یک سیستم اتصال مرکزی (Central Unit)هستند وهر سیستم دارای فضای ذخیره و بازیابی اطلاعات مربوط به خود است. از این رو به اعضاء سیستم Peer یا برابر می گویند.

هر کامپیوتر در این ساختار هم میتواند سرور باشد و هم کاربر یعنی می تواند منابعی را به اشتراک قرار داده و از منابع اشتراکی دیگران استفاده نماید.



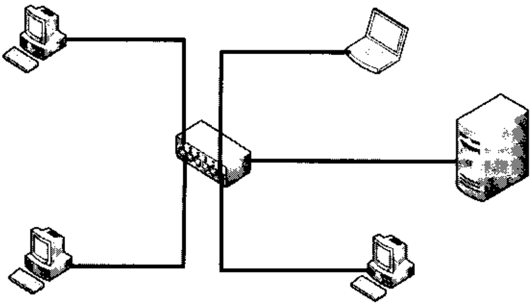
این ساختار خصوصیاتی دارد که به این شرح است:

- هر سیستم باید نسخه پشتیبان از سیستم خود تهیه و ذخیره نماید.
- امنیت شبکه به دلیل عدم وجود یکپارچگی در شبکه در پایین ترین سطح قرار دارد.
- تنها تعداد محدودی کامپیوتر در این ساختار بکار گرفته می شوند.

شبکه های سرور – کاربر

در شبکه های Client –Server یک سیستم عامل شبکه موجود است که وظیفه مدیریت شبکه را از نقطه مرکزی به عهده دارد که همان Server است. تمامی سیستم ها درخواست ها و اطلاعات مورد نیاز خود را به سیستم مرکزی می فرستند. سرور پس از جمع آوری اطلاعات در خصوص این درخواست پاسخ که چگونگی دریافت منابع است را برای کاربر ارسال می کند.

این ساختار مزایای زیادی دارد که به این شرح است:



- این شبکه ها بسیار سازمان یافته تر هستند.
- یافتن منابع در این شبکه بسیار آسان است زیرا در سرور ذخیره شده اند.
- امنیت بالایی دارند.زیرا تمامی کلمات عبور در بانک اطلاعاتی متمرکز در سرور ذخیره می شوند.
- دارای کارایی بالاتری هستندو محدودیتی از نظر تعداد ندارند.

توپولوژی شبکه:

توپولوژی (Topology)در واقع همان ساختار ونقشه شبکه است ونحوه قرارگرفتن سیستم ها در شبکه را مشخص می نماید. کابل ها و تجهیزات مربوط به اتصال در هر نوع توپولوژی بسیار مهم هستند زیرا در هرنوع توپولوژی می بایست از نوع خاصی تجهیزات استفاده نمود که رابطه مستقیم به خواسته ها و انتظارات از اجرای شبکه دارد که در مرحله اجرا بسیار مهم است. یکی از هنر های هر طراح شبکه شناخت توپولوژی و کارکرد آنهاست که در زمان لزوم از کدامیک استفاده نماید.

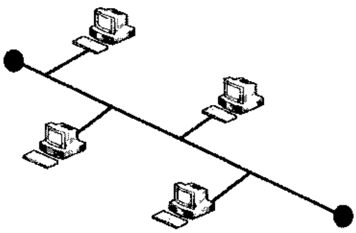
بطور کلی ۴ نوع توپولوژی فیزیکی وجود دارد که به ترتیب ذیل است:

- BUS خطی
- Ring دایره ای
- Star ستاره ای
- Mesh شبکه ای

لازم به ذکر است که در برخی منابع از برخی تعاریف به عنوان انواع دیگر توپولوژی شبکه نام می برند که می توان به Hybrid (ترکیبی از دو توپولوژی مختلف با هم) و Tree(توپولوژی درختی) اشاره نمود که در منابع مورد تایید Comptia از آنها نامی برده نشده است.و تنها به جهت آشنایی شما از آنها نام می بریم.

در ادامه به تفصیل در مورد هرکدام از این توپولوژی ها به تفکیک سخن گفته و مزایا و معایب آنها را بررسی می کنیم.

توپولوژی خطی – BUS



توپولوژی (BUS) یا خطی در این ساختار تمامی کامپیوتر ها به یک کابل سراسری متصل هستند. دو سر این کابل به وسیله ای به نام Terminatorمتصل است.

Terminatorدر واقع یک مقاومت است که مانع برگشت جریان به سیستم می شود و جریان الکتریکی را جذب می نماید. در واقع این نوع توپولوژی ساده ترین نوع است و امروزه کمتر مورد استفاده قرار می گیرد.

مزایا و معایب

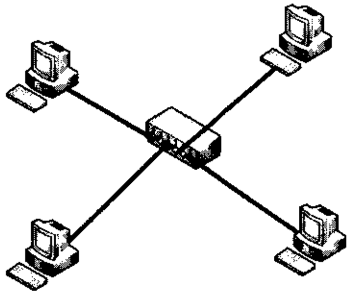
معایب

- انتقال و جابجایی سیستم ها در این ساختار بسیار مشکل است.
- مقاومت این ساختار در برابر مشکلات کم است.با قطع شدن یک سیستم کل شبکه از کار می افتد
- در صورت بروز اشکال عیب یابی و رفع اشکال بسیار مشکل است زیرا نقطه بروز اشکال مشخص نمی باشد.

مزایا

- به آسانی قابل اجرا می باشد
- با هزینه بسیار اندک اجرا می شود(هزینه تجهیزات مصرفی و اجرای آن کم است).
- مصرف کابل شبکه در این ساختار در مقایسه با دیگر توپولوژی ها بسیار کمتر است.

توپولوژی ستاره ای – Star



توپولوژی (Star) یا ستاره ای در این ساختاربر خلاف خطی هر کامپیوتر توسط یک کابل مجزا به نقطه مرکزی متصل می شود. نقطه مرکزی دستگاهی است که با توجه به ساختار و نوع شبکه با یکی از نام های: HUB ,MAU ,Concentrator,Access Point معرفی می گردد.

این ساختار بر خلاف توپولوژی خطی در مقابل مشکلات بسیار پایدار بوده ومعمولترین ساختار شبکه است.

البته در این بخش دو زیر فصل هم باید مورد بررسی قرار گیرد: Point-To-Point وWireless

در ارتباط Point-To-Point سیستم مرکزی یکی از اجزای ارتباط دو طرفه است یعنی کامپیوتر بوسیله کابل به نقطه مرکزی متصل است اما در ارتباط Wireless چون هیچ سیمی وجود ندارد ارتباط مرکزی با دستگاهی به نام Access Point برقرار می شود که وظیفه اتصال را به عهده دارد .حتی در ارتباط ۲ شبکه بدون سیم هم از ساختار ستاره ای استفاده می شود.

مزایا و معایب

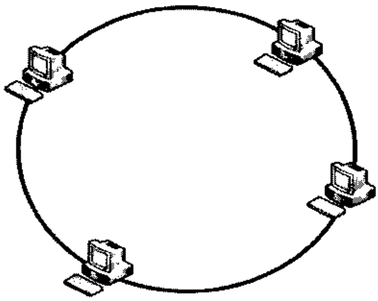
معایب

- هزینه راه اندازی شبکه بسیار گران است چون نیازمند مقدار زیادی کابل شبکه است(اما باتوجه به مزایا ممکن است استفاده از این ساختار به صرفه باشد)
- نقطه ضعف آن سیستم مرکزی(HUB,...) است .با از کار افتادن این بخش کل شبکه از کار می افتد.

مزایا

- اضافه نمودن سیستم های جدید به شبکه به آسانی امکانپذیر است.
- قطع شدن یک سیستم از شبکه تاثیری بر روی شبکه ندارد.
- عیب یابی و رفع اشکال بسیار آسان است.

توپولوژی دایره ای



توپولوژی (Ring) یا دایره ای در این ساختارهر کامپیوتر مستقیم به دو کامپیوتر همسایه خود متصل می شود.در این روش داده ها در یک مسیر یک طرفه از کامپیوتری به کامپیوتر دیگر منتقل می شود.

با توجه به این نکته که کامپیوتر ها با کابل مستقیم به هم متصل می شوند به نظر می رسد ساختن شبکه بسیار آسان باشد اما نکته اینجاست که همانند ساختار خطی هرگونه قطعی یا انتقال و یا جداکردن یک کامپیوتر از شبکه تمام شبکه را دچار اختلال خواهد کرد.چون نیاز است کل شبکه قطع شود تا شما یک سیم را به شبکه اضافه کنید و یا سیستمی را منتقل نمایید.

با توجه به همین دلایل امروزه از این ساختار به ندرت استفاده می شود.

مزایا و معایب:

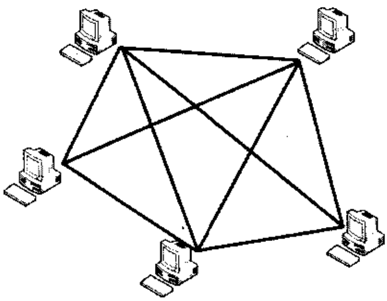
معایب

- دوباره تنظیم کردن شبکه بسیار مشکل است.
- در مقابل مشکلات مقاوم نیست.قطعی یک کابل کل شبکه را مختل می کند.

مزایا

- عیب یابی آن ساده است.زیرا هر سیستم می داند که قطعی از کدام همسایه است که نمی تواند جریان را منتقل کند.

توپولوژی شبکه ای --Mesh

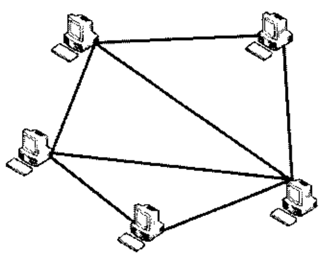


توپولوژی (Mesh) یا شبکه ای در این ساختارین هر دوکامپیوتر یک اتصال مستقیم وجود دارد. به بیان دیگر هر کامپیوتر با تمامی کامپیوترها اتصال مستقیم دارد.واین باعث می شود حداکثر تعداد اتصال به تعداد اجزا سیستم بوجود آید.به همین دلیل پایدارترین ساختار شبکه است و معمولا در شبکه های محلی به ندرت مشاهده می شود.

انواع مختلفی از این ساختار وجود دارد مانند Hybrid-Mesh که در این ساختار بین برخی از کامپیوتر ها تعداد زیادی اتصال وجود دارد که در صد بروز خطا در سیستم را بسیار کم می کند.

حال هرگاه این اتصالات بین تمام اجزا شبکه برقرار شود به آن Full-Mesh می گویند.که این اتصالات برای جایگزینی در هنگام بروز خطا می باشد.تعداد اتصالات برای این ساختار با فرمول n(n-1)/2 محاسبه میشود.

چون با توجه به تعداد بالای کامپیوترها در شبکه ممکن است تعداد اتصالات زیاد شود و مدیریت آنها را سخت نماید ساختار دیگری هم وجود دارد که Partial-Mesh نامیده می شود که اتصال تنها بین برخی اجزا شبکه که لازم است وجود دارد و بقیه اتصالات معمول دارند که معمولترین نوع این ساختار است.



امروزه به ندرت از ساختارشبکه ای استفاده می شود تنها در شبکه های WAN آن هم به دلیل پایداری مورد استفاده قرار می گیرد.

مزایا و معایب:

معایب

- بسیار گران است چون نیازمند اتصالات و کابل زیادی برای هر سیستم است.
- با گسترش شبکه و افزایش سیستم ها تعداد اتصالات زیاد شده ومدیریت ورفع اشکال بسیار دشوار و پیچیده می شود.

مزایا

- در مقابل بروز خطا بسیار مقاوم است. در صورت بروز اشکال و خطا در هر اتصال می توان از اتصالات دیگر برای تبادل اطلاعات استفاده نمود بدون آنکه تاثیری بر شبکه داشته باشد.

انتخاب ساختار مناسب

استفاده از توپولوژی مناسب یک هنر است.که نیازمند تجربه و دانش کافی همچنین شناخت کامل از همه توپولوژی هاست.

مراحل انتخاب توپولوژی می تواند همانند مراحل خرید کفش است.در خرید اندازه وراحتی در کنار بودجه شما فاکتور های اساسی است.

شما با طرح تعدادی سوال می توانید با مناسبترین توپولوژی برسید. سوالاتی مانند:

- چقدر مقاومت در برابر خطا لازم است؟
- چقدر سیستم دچار تغییرات (اضافه کردن سیستم ویا جابجایی و...) می شود که نیازمند دوباره سازی تنظیمات داشته باشد؟
- وسعت مکانی شبکه مورد نظر چقدر است؟
- چقدر هزینه برای راه اندازی شبکه در نظر گرفته شده است؟

رسانه های فیزیکی:

اگرچه امروزه انواع شبکه های بیسیم مانند بلوتوث ، مادون قرمز وفرکانس های رادیویی بسیار محبوب و پرطرفدار شده اند امابرای راه اندازی اکثر شبکه های محلی از کابل های شبکه استفاده می شود.در این بخش به معرفی و شناخت مولفه های کابل های مورد استفاده در شبکه های می پردازیم.

بطور کلی کابل های مورد استفاده به شکل زیر طبقه بندی می شوند:

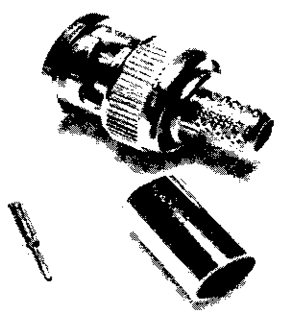
- کابل کوا کسیال(Coaxial Cable)
- کابل های به هم تنیده (Twisted Pair)
- فیبر نوری (Fiber Optic)

کابل کواکسیال(Coaxial Cable)

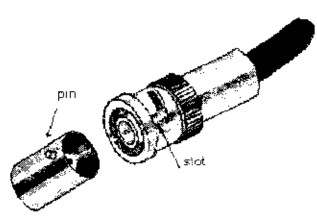
این نوع کابل از یک رسانای مرکزی تشکیل شده که توسط قابی پلاستیکی محافظت می شود.دور این قاب را سیم های افشان پوشانده که همه اینها را محافظی سخت که معمولاً از جنس PV C می باشد احاطه کرده است. لایه محافظ خارجی از جنس عایق نسوز است ودر شرایط بد آب و هوایی هم مقاوم است.

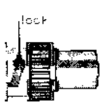
> امروزه با پیشرفت سریع تکنولوژی دیگر به ندرت از این نوع کابل در شبکه استفاده می شود. ولی شما به عنوان یک کارشناس شبکه می بایست از کلیه استانداردها و کابل های شبکه مطلع باشید.

Thin Ethernet:

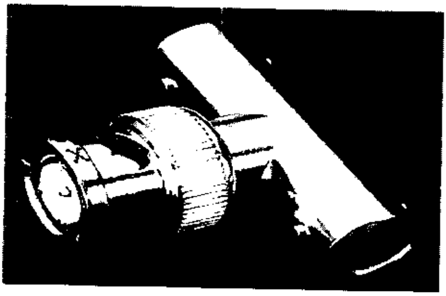


این شبکه همچنین به Thinnet هم مشهور است که در این ساختار کابل 10Base2 مورد استفاده قرار می گیرد.در این نوع کابل از اتصالی با نام BNC استفاده می گردد. در شکل شما این اتصال را مشاهده می نمایید.





دو نوع اتصال BNC وجود دارد نوعی که با پیچ به سیم متصل می شود و نوعی که به سیم پرچ می شود.نوع اول غیر قابل اعتماد است و به سادگی از سیم جدا می شودوکمتر مورد استفاده قرار می گیرد.



هرگاه نیاز باشد که دستگاهی مستقیم به سیم اصلی شبکه (Back Bore)متصل گردد از نوع خاصی اتصال با نام BNC T- Connector استفاده می شود که از نظر ظاهری بسیار شبیه حرف T است.

یاد آوری این نکته ضروری است که پس از اتصال تمامی اجزا به شبکه دو سر آن می بایست به وسیله ای با نام ترمیناتور (Terminator) متصل گردد.

ترمیناتور در واقع یک مقاومت است که مانع بازگشت جریان به داخل سیم می گردد.در صورت عدم وجود این قطعه کل شبکه دچار اختلال می شود.

در این جدول با برخی از استاندارد های کابل کواکسیال آشنا می شوید:

استاندارد کابل	نام مستعار	استاندارد Ethernet	نوع کابل
RG -58U	ندارد	مورد استفاده قرار نمی گیرد	مس سخت
RG-58 A/U	Thinnet	10 Base 2	مس تابیده شده
RG-8	Thicknet	10base 5	مس سخت
RG-62	ARCnet	مورد استفاده قرار نمی گیرد	مس سخت- مس تابیده شده

به خاطر سپردن محتویات این جدول برای آزمون مورد نیاز نیست.ولی در دنیای واقعی شاید شما روزی به این اطلاعات نیاز داشته باشید.این جدول تنها برای اطلاع شما آمده است.

اتصال F:



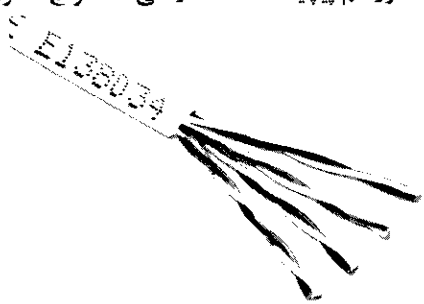
اتصالی است که برای کابل کواکسیال بکار می رود ولی با اتصال BNC متفاوت است این اتصال در کابل هایی با مقاومت ۷۵ Ω بکار می رود حال آنکه در کابل های با مقاومت ۵۰ Ω مورد استفاده قرار می گیرد.در این تصویر اتصال F را مشاهده می نمایید.

کابل های به هم تنیده Twisted Pair :

این کابل از تعدادی سیم مجزا که بصورت زوج هایی به دور هم پیچیده شده اند تشکیل شده است.و با توجه به روکش محافظ آنها به Shielded Twisted Pair)STP)یا کابل روکش دار هم مشهور هستند. که در شبکه های Token Ringمورد استفاده قرار می گیرند.

نوع دیگری هم وجود دارد که فاقد لایه محافظ خارجی است که به آن Unshielded Twisted Pair)UTP) می گویند که در شبکه های اترنت(10Base T و 100 Base TX) مورد استفاده قرار می گیرد.

حال لازم است به بیان این نکته بپردازیم که چرا این کابل ها به دور هم پیچیده شده اند. زمانی که امواج الکترو مغناطیسی درون سیم مسی در جریان هستند،یک محیط مغناطیسی درون سیم ایجاد می شود که باعث بروز تداخلی درون کابل می شود که به آن Cross Talk می گویند.



برای پیشگیری از این عمل سیم ها بصورت دو به دو دور هم پیچیده می شوند که در مقابل این تداخل و سایر عوامل تداخل خارجی مقاوم باشند.

این کابل ها معمولترین کابل در شبکه های امروزی بوده وبه دلایل زیر بسیار پرطرفدار هستند:

- از دیگر انواع کابل ها ارزانتر هستند
- کارکردن با آنها بسیار ساده است.
- این کابل ها امکان انتقال اطلاعات تاچندین برابر ظرفیت کابل های قدیمی را میسر می سازند.

این کابل ها به شاخه های (Category) تقسیم بندی می شوند:

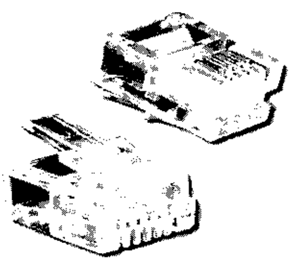
- دسته اول(Category1):از دو زوج سیم (چهار رشته)تشکیل شده و برای انتقال صوت در شبکه های تلفن بکار می رود و در شبکه کاربردی ندارد.
- دسته دوم (Category2) :از چهار زوج سیم (هشت رشته)تشکیل گردیده که امکان انتقال اطلاعات تا حداکثرMbps ۴ را دارا می باشد.
- دسته سوم (Category3) :همانند دسته قبلی از ۸ رشته تشکیل شده که امکان انتقال داده ها تا MHZ۱۶ را دارد.این دسته در دهه ۸۰ میلادی بسیار پرطرفدار بوده و لی امروزه کاربرد چندانی ندارد.
- دسته چهارم (Category4) :از ۴ زوج سیم تشکیل شده و امکان انتقال تا MHZ۲۰ را فراهم می آورد.

- دسته پنجم (Category5) :همانند دسته های قبلی از ۴ زوج تشکیل یافته و امکان انتقال تا MHZ۱۰۰ را فراهم م آورد.البته یک زیر شاخه هم دارد که Category5e نامیده می شود. با توجه به این که در این حالت هر زوج می تواند ارسال و دریافت اطلاعات نماید می توان برای شبکه های GB(Giga bit) از این کابل استفاده نمود.
- دسته ششم (Category6) :این استاندارد در سال ۲۰۰۲ بوجود آمده و امکان انتقال داده ها تا MHZ ۲۵۰ را دارد.

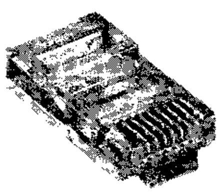
> در دنیای واقعی گاهی به جای کلمه Category از مخفف آن Cat استفاده می شود.
> قبل از انتخاب کابل شما می بایست تجهیزات مورد استفاده در شبکه را مورد بررسی قرار دهید. کابل شما می بایست با حداقل های شبکه شما همخوانی داشته باشد و آینده نگری در مورد نیاز های آینده شبکه هم مورد نظر قرار گیرد.

حال که شما انواع کابل های UTP را شناختید به سراغ نحوه استفاده و اتصال آن به دستگاه های مختلف می رویم.

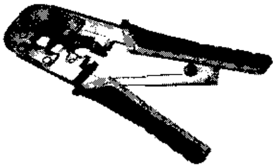
اتصال کابل UTP:



همانطور که می دانید اتصالBNC را در این نوع کابل ها نمی توان بکار برد.برای این کابل ها اتصالی با نام RJ (Registered Jacket) مورد استفاده قرار می گیرد.کابل تلفن از اتصالی به نام RJ-11 استفاده می نماید که از ۲ زوج استفاده می کند تفاوت آن در ظاهر آن است.



جهت اتصال کابل شبکه نیز از اتصالی با نام RJ-45 استفاده می شود.که از هر ۴ زوج استفاده می شود که ترتیب قرارگرفتن سیم ها درون اتصال مهم است که در بخش های آتی به آن خواهیم پرداخت



برای آماده سازی کابل و اتصال از دستگاهی با نام Crimper کمک گرفته می شود.با کمک این ابزار می توان اتصال RJ را به کابل شبکه متصل نمود.این اتصال ها تنها یکبار به کابل متصل می شود.

کابل های اترنت (Ethernet):

این کابل ها با کد های مخصوصی معرفی می شوند و در شبکه های اترنت مورد استفاده قرار می گیرند. کد ها از این قاعده کلی تبعیت می کنند: N<signaling>-X

که بخش اول سرعت انتقال را نمایش می دهد. بخش دوم نام آن است و بخش سوم نام منحصر به فرد مربوط به نام کابل است.

به عنوان مثال ، 10Base-FL نشان دهنده سرعت انتقال ۱۰ و نوع کابل فیبر نوری می باشد .

شما در این جدول با تمامی مشخصات انواع کابل های اترنت آشنا می شوید:

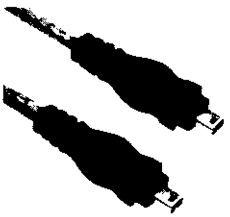
نام	نوع کابل	حداکثر سرعت	حداکثر فاصله موثر
10Base5	Coax	10Mbps	500 meters
10Base2	Coax	10Mbps	185 meters
10Base-T	UTP	10Mbps	100 meters
100Base-TX	UTP,STP	100Mbps	100 meters
10Base-FL	Fiber	10Mbps	Between 500 to 2000 meters
100Base-FX	Multimode Fiber	100Mbps	2000 meters
1000Base-T	UTP	1000Mbps	100 meters
1000Base-SX	Multimode Fiber	1000Mbps	550 meters
1000Base-CX	Balanced shielded copper	1000Mbps	25 meters
1000Base-LX	Multimode&single mode fiber	1000Mbps	550 meters MMF 2000 meters SMF
10GBase-SR	Multimode Fiber	10Gbps	300 meters
10GBase-LR	Single- mode fiber	10Gbps	10kilometers
10GBase-ER	Single- mode fiber	10Gbps	40kilometers
FDDI	Multimode Fiber	100Mbps	10kilometers

انواع دیگر کابل های شبکه:

کابل (i-Link) یا IEEE1394 یا (Fire Wire):

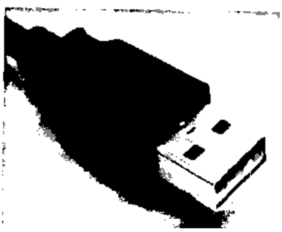
این کابل نوعی منحصر به فرد از کابل است که برای مقاصد خاصی استفاده می شود. قابلیت انتقال اطلاعات با سرعت های ۸۰۰،۴۰۰،۲۰۰،۱۰۰ مگابیت بر ثانیه را دارد.استفاده از این کابل ها محدود بوده و عمدتا برای انتقال اطلاعات بین دو کامپیوتر کنار هم ویا بین دستگاه های دیجیتالی صوتی و کامپیوتر مورد استفاده قرار می گیرد.

اتصال این نوع کابل بر دو گونه است: Pin۴ وPin ۶
اتصال Pin۶ زمانی بکار می رود که نیاز به انتقال جریان لکتریسیته از کامپیوتر به دستگاه دیگری لازم باشد. برای کسب اطلاعات بیشتر می توانید به وب سایت WWW.1394ta.org مراجعه نمایید.


4 pin


6 pin

کابل USB (Universal Serial Bus):



در سال های اخیر این اتصال جای اتصال های قدیمی در کامپیوتر ها را گرفته است. محدوده عملکرد این اتصال بسیار وسیع و بسیار قابل انعطاف می باشدو امروزه تجهیزات زیادی با این اتصال وجود دارند.

این اتصال می تواند جریان اکتریسیته را منتقل نموده و از هر درگاه امکان استفاده همزمان ۱۲۷ وسیله وجود دارد. (بوسیله هاب)

کابل های فیبر نوری:

فیبر نوری برای انتقال اطلاعات از نور بجای جریان الکتریکی استفاده می کند. از همین رو در مقابل اختلالات الکترو مغناطیسی و امواج رادیویی بسیار مقاوم است.ذکر این نکته ضروری است که بروز اختلال علیرغم مقاومت فیبر نوری ممکن است در کارایی شبکه تاثیر منفی داشته باشد.

فیبر نوری از یک هسته مرکزی از جنس شیشه یا پلاستیک تشکیل شده است.استفاده از شیشه فاصله موثر انتقال نور را افزایش می دهد.استفاده از پلاستیک قیمت فیبر راکاهش می دهد. صرفنظر از جنس هسته مرکزی ،در نوع عملکرد تاثیری ندارد.

فیبر ها در دو نوع کلی وجود دارند:

- SMF(Single Mode Fiber)
- MMF(Multi Mode Fiber)

تفاوت عمده این دونوع با هم در تعداد اشعه های نوری است که در هر لحظه می توانند منتقل نمایند.

MMF برای انتقال در فواصل کوتاه و SMF برای فواصل طولانی بکار می رود. برای شناخت این دو نوع از هم دو راه ساده وجود دارد:

- اگر نوار زرد رنگ روی بدنه خارجی فیبر بود SMF است و اگر نوار نارنجی رنگ باشد MMF است.
- اگر روی بدنه اعداد ۶۲.۵/۱۲۵ نقش بسته بود (که بیانگر قطر خارجی فیبر است) فیبر از نوع MMF است و اگر شماره های ۸،۹ ویا ۱۰ بود فیبر از نوع SMF است.

مزایا ومعایب استفاده از فیبر نوری:

مزایا:

- بسیار مقاوم در برابر اختلالات اکتریکی و الکترو مغناطیسی می باشد.
- می تواند داده ها را تا فاصله ۴۰ کیلومتری منتقل نماید.

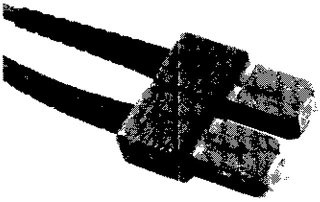
معایب:

- نصب و راه اندازی آن بسیار دشوار است.
- خرید تجهیزات و راه اندازی این شبکه نیازمند سرمایه گزاری هنگفتی است.

اتصال های فیبر نوری:

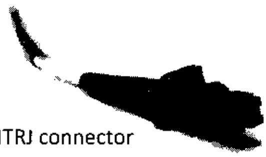


فیبر از اتصالات خاصی استفاده می کند که ST(Straight Tip) و(Square SC (Connector می باشد.اتصال ST بیشتر مورد استفاده قرار می گیرد.سیستم اتصال بسیار شبیه به BNC می باشد.

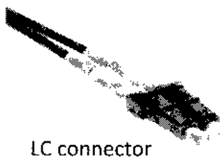


نوع دیگر اتصال SC می باشد که د ارای یک گیره کوچک است که پس از متصل شدن مانع خروج بی دلیل آن می شود . آن را قابل اعتماد می نماید.این اتصال برای هر دونوع فیبر نوری مورد استفاده قرار می گیرد ولی محبوبیت آن از ST کمتر است.

انواع دیگر اتصال های فیبر نوری با عنوان SFF(Small Form Factory) می باشند.که چون اندازه ای بسیارکوچک دارند می توان تعداد زیادی از آنها را در کنار هم استفاده نمود.که به دو شکل LC(Local Connector) و MTRJ(Mechanical Transfer Registered Jack) موجود هستند.



MTRJ connector



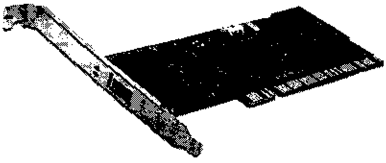
LC connector

تجهیزات ارتباطی شبکه:

پس از آنکه با رسانه های فیزیکی شبکه آشنا شدید حال نوبت شناخت برخی تجهیزات که امروزه در شبکه ها به کار می روند می رسد. این تجهیزات به تجهیزات ارتباطی شبکه مشهور هستند.

- کارت شبکه Network NIC
- هاب HUB
- سوئیچ SWITCH
- پل ارتباطی Bridge
- مسیریاب Router
- دروازه Gateway
- تجهیزات دیگر

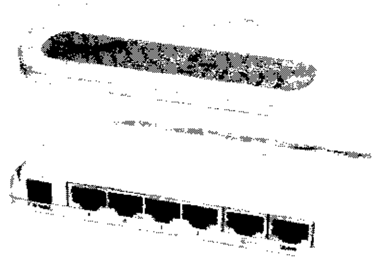
کارت شبکه Network NIC



وسیله ای است که ارتباط فیزیکی و الکترونیکی کامپیوتر با شبکه را میسر می سازد.معمولاً هر کارت شبکه دارای ۲ چراغ است یکی برای نشان دادن اتصال کابل و دیگری نمایش میزان فعالیت در شبکه.

هاب HUB:

همانطور که قبلا آموختید در توپولوژی ستاره ای همه سیستم ها بوسیله کابل های مجزا به نقطه مرکزی که همان HUB بود متصل می شدند. و HUB وظیفه اتصال اجزا به هم را بر عهده داشت.عملکرد HUB بدن صورت است که هر داده ای که به آن می رسد؛آن را برای تمامی سیستم های شبکه ارسال می کند تا به دست گیرنده اصلی برسد.در واقع HUB مکانیزمی برای شناسایی گیرنده ندارد.این عمل باعث ایجاد اختلالی با نام (Collision)یا تصادف میگردد. HUB تنها می تواند اتفاق افتادن این پدیده را نظاره کند CSMA/CD (Collision Detection/ Carrier Sence Multiple Access)وامکان جلوگیری و رفع این اختلال را ندارد.



بصورت خلاصه می توان گفت : هاب تنها یک تکرار کننده است که داده را تکرار کرده تا به دست گیرنده برسد.به همین دلیل امروزه به ندرت از آن استفاده می شود.

سوئیچ SWITCH :

این وسیله هم همانند هاب وظیفه اتصال اجزا شبکه را برعهده دارد.و لی بر خلاف هاب ، بر اساس آدرس فیزیکی گیرنده (MAC Adress)،داده را مستقیم و تنها برای گیرنده ارسال می نماید.



برتری عمده سوئیچ بر هاب کارایی وکیفیت بالاتر است.

پل ارتباطی Bridge:

وسیله ای است که برای اتصال دو شبکه همسان را به هم متصل می نماید.یکی از مزایای استفاده از این دستگاه تقسیم کردن شبکه ای شلوغ به دو بخش و محدود کردن ترافیک هر بخش به همان قسمت می باشد.

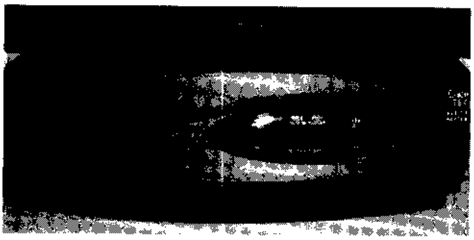


تنها زمانی اجازه عبور ترافیک داده می شود که فرستنده یک طرف باشد و گیرنده در طرف دیگر باشد.

مسیریاب Router :

دستگاهی است بسیار پیچیده که دو یا چند شبکه غیر همسان را به هم متصل می نماید.این دستگاه پس از دریافت داده ها و استخراج آدرس مقصد آنها طی فرآیندی پیچیده می تواند بهترین مسیر برای ارسال آن به مقصد را تعیین نماید.

این دستگاه همانند یک کامپیوتر در مقیاس کوچکتر می باشد.دارای پردازشگر(CPU)برای پروسه تعیین مسیر و یک سیستم عامل (مثلاً در سیسکو IOS)هستند.



با توجه به توان بالای این دستگاه می توان آن را برای مقاصد دیگری مانند دیواره آتش(Fire Wall)و دروازه سیستم (Gateway) هم پیکر بندی و مورد استفاده قرار داد.

دروازه خروجی Gateway

تلفیقی از سخت افزار و نرم افزار بوده و وظیفه اتصال دو یا چند شبکه با ساختار متفاوت رابر عهده دارد.به عنوان مثال فرض کنید یک شبکه محلی با کامپیوتر های شخصی را بخواهید با شبکه ای از ابر کامپیوتر ها(Mainframe Computers) متصل نمایید. وظیفه دروازه اینجا آشکار می شود که باید داده ها به صورتی در آیند که قابل فهم و استفاده برای هر کدام از این شبکه ها باشد.

تجهیزات ارتباطی دیگر:

علاوه بر این تجهیزاتی که ذکر شد،دستگاه های دیگری نیز وجود دارد که شاید مستقیم متصل به شبکه نباشند اما در چرخه شبکه نقش مهم و ضروری دارند.

- مودم Modem
- ISDN Terminal Adapter
- Wireless Access Point
- CSU/DSU
- Transceivers
- Firewalls

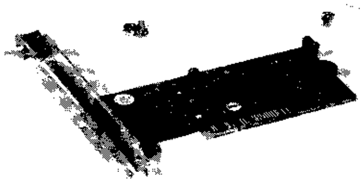
مودم Modem

دستگاهی است که داده های دیجیتال را به آنالوگ تبدیل نموده تا قابل ارسال از طریق رسانه فیزیکی آنالوگ گردند،پس از رسیدن به مقصد مجدد آنها را به داده های دیجیتال تبدیل می کند.

هرگاه از مودم سخن می گوییم منظور ما یکی از این ۳ نوع می باشد:

- مودم خطوط آنالوگ (POTS)
- مودمDSL
- مودم کابلی(Cable Modem)

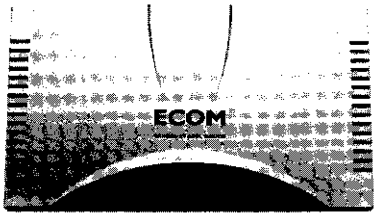
مودم خطوط آنالوگ (POTS)



این مودم در اکثر کامپیوتر های امروزی مشاهده می شود.و برای اتصال به شبکه از طریق خطوط تلفن آنالوگ یا همان شبکه تلفن شهری استفاده می شود.

مودمDSL:

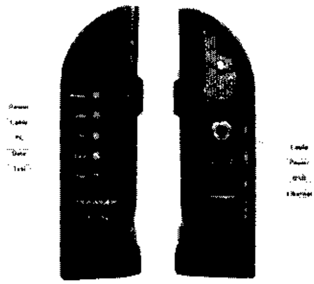
خطوط DSL (Digital Subscriber Line) بسرعت جای خطوط آنالوگ را می گیرد. چون سرعت بالاتری را به هزینه ای اندک فراهم می آورد. همچنین شما می توانید تماس تلفنی برقرار کنید همزمان هم می توانید از شبکه استفاده نمایید.



زیرا شبکه از فرکانس ۳۲۰۰ و بالاتر استفاده می کند و تلفن از فرکانس پایین تر استفاده می کند پس هیچ تداخلی ایجاد نمی شود.

هرگاه شما بخواهید از شبکه و تلفن بصورت همزمان استفاده نمایید ، می بایست از یک فیلتر ویژه استفاده نمایید.که به آن جداکننده یا (Splitter) می گویند.در غیر اینصورت در هنگام مکالمه تلفنی صدایی مانند "هیس" می شنوید.

مودم کابلی(Cable Modem):



این سرویس برروی شبکه تلویزیون کابلی که در اکثر کشور ها فعال است قراردارد.یعنی شما با کمک یک مودم کابلی هم به تماشای تلویزیون بپردازید و هم از سرویس شبکه برخوردار شوید.

این شبکه از کابل کواکسیال برای انتقال جریان استفاده می کند.

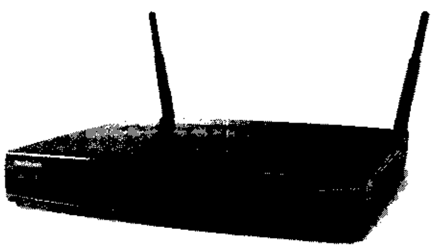
مبدل ISDN (ISDN Terminal Adapter):

خطوط (ISDN) نوع دیگری از شبکه های پرسرعت است. این شبکه داده ها را با سرعت بالاتر از ۶۴ کیلوبایت در ثانیه منتقل می نماید.

ISDN Terminal Adapter یک مودم نیست چون تغییری از آنالوگ به دیجیتال انجام نمی شود بلکه فرمت دیجیتال با این دستگاه تغییر می کند.

نقطه دسترسی بیسیم (Wireless Access Point)WAP:

این د ستگاه به کاربران متحرک اجازه می دهد به شبکه متصل شوند و از منابع اشتراکی یک شبکه کابلی استفاده نمایند.یک سمت این دستگاه شبکه ای بیسیم است وسوی دیگر به یک شبکه با سیم متصل است.



به معنای دیگر این وسیله معادل بیسیم هاب یا سوئیچ است.یکی از کاربردهای این وسیله ارایه دسترسی به اینترنت درمکان های عمومی مانند کتابخانه،فرودگاه و هتل ها می باشد.

CSU/DSU:

دستگاهی است با نام کامل Channel Service Unit/Data Service Unit که در تمامی اتاق های سرور یافت می شود هرگاه از خوط دیجیتالی(T-Series) استفاده شود.این دستگاه خطوط دیجیتال را به شبکه (مسیریاب)متصل می کند.



این دستگاه دارای تعدادی چراغ است که می توان وضعیت خط را کنترل نمود.جهت ارتباط این دستگاه بامسیریاب معمولا از کابل v.35استفاده می شود.

Transceivers(Media Converters) تبدیل کننده رسانه:



یکی از تجهیزات کوچک شبکه است که کاربرد اصلی آن برای اتصال کارت شبکه و یاهر دستگاه دیگری به رسانه ای که برای آن ساخته نشده است. به عنوان مثال فرض کنید شما دو سوئیچ 100Base-TX در اختیار دارید و می خواهی این دو را بوسیله فیبر نوری به هم متصل نمایید.شما یک تبدیل کننده رسانه(Media Converters) به هرکدام از این سوئیچ ها متصل می نماییدو سپس این دو تبدیل کننده را با فیبر نوری مناسب به هم متصل می نمایید.

Firewalls(دیواره آتش):



هرگاه نیاز باشد که شبکه شما به اینترنت متصل شود،مهمترین وسیله یک دیواره آتش در آخرین نقطه شبکه است. وظیفه این دستگاه محافظت کاربران شبکه داخلی و منابع داخلی از گزند سارقین اینترنتی است.

ممکن است برای این منظور شما دستگاهی مجزا خریداری نمایید و یا بصورت نرم افزاری یک دیواره آتش ایجاد نمایید.پیکر بندی صحیح دیواره آتش بسیار مهم است.زیرا خط مقدم در برابر حملات اینترنتی است.

همچنین شما می توانید مانع دسترسی کاربران داخل شبکه به برخی منابع اینترنت هم شوید.انتخاب سخت افزار و نرم افزار نیاز به شناخت مواردی دارد که در مباحث بعدی به آن می پردازیم.

جمع بندی:

در این بخش شما:

- ❖ **با انواع توپولوژی های شبکه آشنا شدید.**
- ❖ **با مولفه های انواع کابل های شبکه آشنا شدید.**
- ❖ **پس از مطالعه مطالب این فصل می توانید انواع اتصال شبکه را شناسایی نمایید.**
- ❖ **با انواع رسانه های فیزیکی شبکه آشنا شدید.**
- ❖ **با نحوه عملکرد و کارکرد تجهیزات شبکه آشنا شدید.**

سوالات ارزیابی برای آزمون Network+ :

۱- کدامیک از این گزینه ها خصوصیات شبکه یک- به -یک را توصیف می نماید.(تمامی موارد صحیح را مشخص نمایید)

الف) مدیریت متمرکز بر شبکه انجام می شود.
ب) هر سیستم می تواند کاربر یا سرور باشد.
ج) تعداد سیستم ها در این ساختار محدود است.
د) نیاز به هاب یا سوییچ ندارد.

۲-.کدامیک از این رسانه ها می توانند ۱۰۰۰ مگابیت در ثانیه را منتقل نماید.
الف)10Base-T
ب) 100Base-TX
ج) 1000Base-TX
د) 10GBase-SR

۳-.کدامیک از این اتصال ها در فیبر نوری مورد استفاده قرار می گیرد. .(تمامی موارد صحیح را مشخص نمایید)
الف) BNC
ب) MTRJ
ج) RJ-45
د) SC

۴- کدامیک از چراغ های وضعیت بر روی کارت شبکه می تواند اولین نشانه برای عیب یابی را نمایش می دهد.
الف) چراغ برقراری ارتباط شبکه
ب) چراغ نمایش تصادف در شبکه
ج) سرعت اتصال شبکه (100/10)
د) چراغ فعالیت شبکه

۵-کدامیک از این موارد از مزایای ساختار شبکه ای یا Mesh می باشد. .(تمامی موارد صحیح را مشخص نمایید)
الف) هزینه کابل کشی را کاهش می دهد.
ب) ارتباط بین اجزای شبکه را قابل اعتماد می سازد .
ج) میزان کابل شبکه را کاهش می دهد.

د) نیاز به یک توکن برای برقراری ارتباط دارد.

۶- کدامیک از این موارد از مزایای ساختار ستاره ای یا Star می باشد. (تمامی موارد صحیح را مشخص نمایید)

الف) حجم کابل شبکه مصرفی را کاهش می دهد.

ب) در صورت بروز اختلال در سیستم تنها همان سیستم دچار اختلال می شود.

ج) تنها یک نقطه وجود دارد که در صورت بروز اشکال تمام شبکه را مختل می کند.

د) عیب یابی و رفع اشکال در این ساختار بسیارساده تر از دیگر ساختار ها می باشد .

۷-در کدام اتصال انرژی برق هم می تواند منتقل شود. (تمامی موارد صحیح را مشخص نمایید)

الف) USB

ب) Firewire 4 pin

ج) Firewire 6 pin

د) کابل کواکسیال

۸-کدامیک از تجهیزات زیر می تواند برای تبدیل نوع کابل ارتباطی مورد استفاده قرار گیرد. .

الف) پل ارتباطی

ب) مبدل رسانه

ج) مسیریاب

د) سوییچ

۹- در ساختار Cat 5 و اتصال RJ-45 چند زوج کابل مورد استفاده قرار می گیرد.

الف) ۲

ب) ۳

ج) ۴

د) ۸

۱۰- برای حفظ امنیت شبکه داخلی ازتهدیدات بیرون شبکه ؛ کدامیک از تجهیزات زیر استفاده می شود.

الف) مسیریاب

ب) سوییچ

ج) دیواره آتش یا فایروال

د) پل ارتباطی

پاسخ به سوالات این بخش

۱ - **ب ؛ ج ؛ د**

سیستم ها در این ساختار می توانند کاربر یا سرور باشند.

تعداد کاربران در این ساختار محدود است.

این ساختار نیاز به هیچ دستگاه مرکزی مانند هاب یا سوییچ ندارد.

۲ - **ج**

10Base-T سرعت ارتباط ۱۰ مگابیت است

100Base-TX سرعت ارتباط ۱۰۰ مگابیت است

10GBase-SR سرعت ارتباط ۱۰ گیگابیت است

۳ - **ب ؛ د**

BNC در کابل کواکسیال مورد استفاده قرار می گیرد.

RJ-45 در کابل های UTP استفاده می شود.

۴ - **الف**

مهمترین مورد در این حالت برقراری ارتباط است. قبل از برقراری ارتباط موارد دیگر اهمیتی ندارد.

۵ - **ب**

هزینه کابل شبکه در این ساختار افزایش می یابد.

میزان کابل مصرفی بسیار افزایش می یابد.

توکن در ساختار دایره ای استفاده می شود.

۶ - **ب ؛ ج ، د**

حجم کابل مصرفی در مقایسه با ساختار های دایره ای و خطی بسیار بیشتر است.

۷ - **الف ؛ ج**

Firewire 4 pin نمی تواند برق رامنتقل نماید

کابل کواکسیال هم نمی تواند برق را منتقل نماید.

۸ - **ب**

پل ارتباطی برای برقراری ارتباط منطقی بین اجزای شبکه مورد استفاده قرار می گیرد.

مسیریاب برای مسیریابی بین اجزای شبکه بکار می رود.
سوییچ برای برقراری ارتباط فیزیکی بین اجزا شبکه می باشد.

۹ -ج

در این ساختار از ۴ زوج و ۸ رشته مورد استفاده قرار می گیرد.

۱۰ ج

علاوه بر دیواره آتش مسیریاب هم می تواند برای تامین امنیت بصورت ویژه ای پیکربندی شود. اما چون یک پاسخ مورد نظر است ؛پاسخ صحیح گزینه " ج " است.

فصل دوّم

مدل OSI



شما در این فصل با این مفاهیم آشنا خواهید شد:

۱-۲ شناسایی مشخصات و مولفه های 802.2 (کنترل منطقی خط)، 802.3 (اترنت)، 802.5(توکن رینگ)،802.11 (شبکه وایرلس) و شبکه های فیبر نوریFDDI مانند:

- سرعت
- طریقه دسترسی (CSMA/CA)و (CSMA/CD)
- توپولوژی
- رسانه

۲-۲ شناسایی آدرس فیزیکی شبکه (MAC)و اجزاء آن

۳-۲ شناسایی ۷ لایه مدلOSI و عملکرد هر لایه

۴-۲ معرفی تجهیزات شبکه به تفکیک لایه عملکرد هر کدام

تجهیزاتی مانند:

- هاب
- سوییچ
- پل ارتباطی
- مسیریاب
- کارت شبکه
- نقطه دسترسی بیسیم

۵-۲ شناسایی تفاوت های پروتکل های شبکه از نظر مسیریابی ،آدرس دهی ، ارتباط داخلی ونامگذاری در پروتکل های:

- IPX/SPX
- NetBEUI
- Apple Talk/Apple Talk Over IP
- TCP/IP

مقدمه:

یر ممکن است شما کتابی در مورد شبکه پیدا کنید که در مورد مدل OSI مطلبی ننوشته باشد.این کتاب هم استثنا یست. این مدل به شما کمک می کند که مبانی شبکه را بشناسید و همچنین چگونگی ارسال داده ها از یک کامپیوتر به کامپیوتر دیگر را مشخص می نماید.

علاوه بر مدل OSI ما در خصوص پروتکل ها و نحوه عملکرد آنها و همچنین تجهیزات مورد استفاده در شبکه ها به تفکیک لایه ها بحث خواهیم نمود.

مدل OSI چیست؟

موسسه جهانی استاندارد ISO(International Standard Organization) برای یکسان سازی عملکرد ها و ارایه یک طرح جامع اقدام به طراحی و معرفی استانداردی به نام OSI (Open System Interconnect) نموده است که تمامی سخت افزار ها و نرم افزار های شبکه باید از این استاندارد تبعیت نمایند.

علاوه بر این نحوه تعامل بین اجزاء شبکه نیز در این استاندارد تعیین شده است.بسیاری از پروتکل ها تنها برای اجرای یک هدف که آن هم انتقال داده ها در شبکه است بوجود آمده اند.

پروتکل چیست؟

پروتکل مجموعه ای از قوانین و قرارداد هایی می باشد که نحوه تعامل تجهیزات و سیستم های مختلف با هم را مشخص می نماید.

پروتکل همانند "زبان "عمل می کند،اگر فردی بخواهد با زبان فارسی با فرد دیگری که زبانش انگلیسی است گفتگو کند آیا امکانپذیر است؟ واضح است که خیر مگر آنکه به زبان سومی که هردو به آن تسلط هستند گفتگو انجام شود.

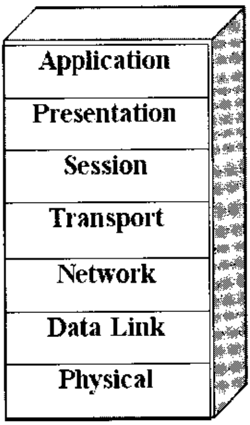
بسته قوانین یا Protocol Stack :

Protocol Stack یا" مجموعه پروتکل " تعدادی پروتکل همسان هستند که با کمک هم می توانند برقراری ارتباط و تبادل داده ها را ممکن سازند.

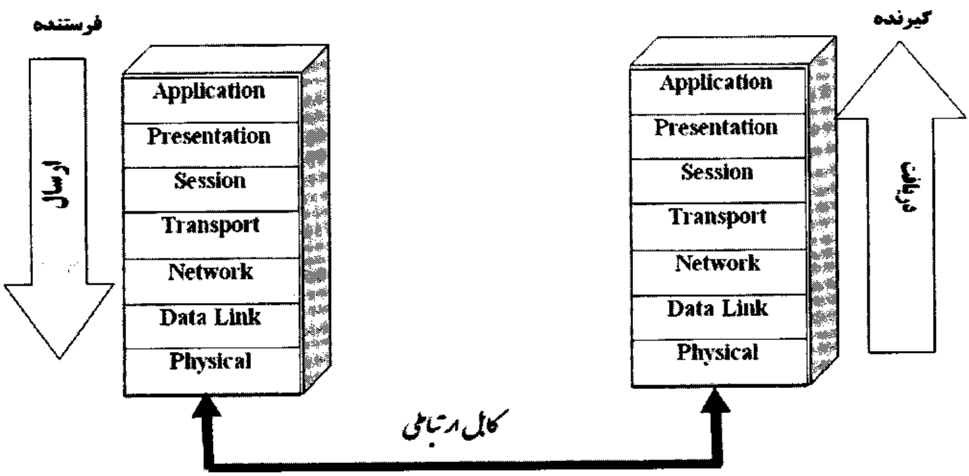
مدل OSI سعی دارد که بیان کننده نوع انتقال داده از لایه های فیزیکی و رسیدن آن به مقصد با فرم اصلی آن باشد.به بیان دیگر یک داده به چه فرمتی تبدیل می شود تا از لایه فیزیکی عبور کند و مجدد، در مقصد به صورت داده در آید تا قابل استفاده در سیستم مقصد باشد.

مزیت اصلی این مدل تقسیم بندی دقیق بین عملکرد بخش های مختلف سیستم است که با تعداد زیاد این لایه ها امکانپذیر شده است.

در تصویر زیر شما شمای کلی این مدل را مشاهده می نمایید:



همانگونه که شما در تصویر مشاهده می نمایید، مدل OSI به هفت لایه تقسیم شده است.در هر لایه اعمال خاصی بر روی داده انجام می شود و داده به لایه بعدی ارسال می شود.



هنگام ارسال داده ها در یک سیستم، داده ها از لایه هفتم (بالاترین لایه) به سمت پایین حرکت نموده تا به کابل ارتباطی رسیده و از این طریق به مقصد برسد. اما در سیستم مقصد،از لایه اول (پایینترین لایه) شروع می شود که در تصویر مشاهده می نمایید.

این ارتباط صرفنظر از نوع سیستم عامل تنها با استفاده از پروتکل یکسان قابل اجرا است.در این فرآیند داده ها طی فرآیند خاصی بسته بندی (Encapsulation) می شوند که تبادل آنها ساده تر گردد.این بسته ها تنها توسط سیستم دیگری که از پروتکل یکسان با فرستنده بهره می برد قابل بازگشایی و استفاده بوده و یا توسط مسیر یاب ها قابل انتقال است.

ترتیب این لایه ها مهم است و شما باید نام و ترتیب این لایه ها را به خاطر بسپارید.

مشخصات لایه ها :

در این بخش شما با مشخصات و عملکرد هر لایه به تفکیک آشنا می شوید:

لایه هفتم: لایه کاربردی یا Application

این لایه بالاترین لایه در این مدل است و برقرارکننده ارتباط کاربر با شبکه و سیستم است.در این لایه سرویس های مورد نیاز کاربر قرار دارد و اعمالی مانند بازیابی خطاهای احتمالی و ارایه سرویس های مختلف مانند چاپ هم در این لایه انجام می گیرد.

در واقع در نگاه اول به نظر می رسد که مثلا در هنگام کار با مرورگر صفحات اینترنت،این نرم افزار هم در این لایه قرار دارد.ولی این نرم افزار تنها از پروتکل HTTP(Hyper Text Transfer Protocol) برای دریافت و نمایش صفحات اینترنت کمک می گیرد و بدون این پروتکل ها هیچ عملکردی ندارد.

لایه ششم :لایه نمایش یا Presentation

در این لایه اعمالی مانند تغییر فرمت نمایش کاراکتر ها ،رمز گشایی و رمز نگاری،فشرده سازی در این مرحله انجام می شود.

همچنین فرمت داده های دریافتی تشخیص داده می شود و مشخص می شود این داده توسط کدام نرم افزار کاربردی قابل اجرا و بهره برداری است.این عمل از روی پسوند داده ها (.jpg,.mpg,.mid,.txt)مشخص می شود.

لایه پنجم: لایه جلسه یا Session

در این مرحله مشخص می شود که دو کامپیوتر چگونه ارتباط خود را آغاز نموده،داده ها را منتقل وارتباط را قطع نمایند.به این مرحله از آغاز تا پایان یک (Session)یا جلسه می گویند.

مراحل امنیتی مانند بررسی مجوز عبور (Authentication)،اجازه انتقال داده ها و خاتمه دادن ارتباط هم در این لایه انجام می پذیرد.

لایه چهارم: لایه انتقال یا Transport

در این لایه بررسی می شود که آیا داده های منتقل شده بصورت کامل و صحیح منتقل شده اند و خطایی در ارسال آنها رخ نداده است.

در این لایه پیام های بلند برای سهولت ارسال به بخش های کوچکتری تقسیم می شود به لایه سوم ارسال شده و تکه های کوچک پیام به صورت اولیه درآمده و به لایه پنجم ارسال می گردد.

در این لایه دو نوع پروتکل وجود دارد :

- پروتکل وابسته به اتصال (Connection Oriented)
- پروتکل مستقل از اتصال (Connectionless)

تفاوت این دو نوع پروتکل در این نکته است که پروتکل وابسته به اتصال پس از انتقال داده به گیرنده بررسی می کند که آیا به درستی انتقال انجام شده است.در صورت بروز مشکل داده را مجدد ارسال می نماید و پس از صحت انتقال داده های دیگر را منتقل می نماید.اما در پروتکل مستقل از اتصال تنها ارسال مهم است .

لایه سوم: لایه شبکه یا Network

در این لایه آدرس های منطقی (Logical) به آدرس های فیزیکی (Physical) تبدیل شده تا آماده ارسال در شبکه شوند. در این لایه همچنین اولویت بندی داده ها (Prioritization) انجام میگیرد.فرض کنید که شما منتظر یک نامه الکترونیکی هستید تاخیر ۲ دقیقه ای در ارسال شما را خیلی ناراحت نمی کند اما اگر در حال دیدن یک فیلم هستید تاخیر ۲ دقیقه ای شما را خیلی عذاب می دهد. به همین دلیل است که از اولویت بندی استفاده می شود.

لایه دوم : لایه انتقال داده ها یا Data Link

در این لایه داده هایی که از لایه های بالاتر ارسال شده اند در یک بسته منطقی با نام (Frame) قرار داده می شوند و آماده ارسال در شبکه می گردند.

لایه اول : لایه فیزیکی یا Physical

در این لایه نوع کابل ،انواع اتصال و تکنولوژی های ارتباطی مورد بحث قرار می گیرد.این لایه برقرار کننده ارتباط فیزیکی با شبکه است.

به نسبت اهمیت بحث و همچنین نزدیکی عملکرد برخی لایه ها به هم این مدل را به ۳ قسمت تقسیم می نماییم:

- لایه های پایینی شامل لایه های اول و دوم
- لایه های میانی شامل لایه های سوم و چهارم
- لایه های بالایی شامل لایه های پنجم ،ششم و هفتم

ال به تفکیک به توضیح هر کدام می پردازیم.

یه های پایینی مدل

یه اول: Physical

ر این لایه ها تجهیزات چیزی از محتوای داده هایی که منتقل می شود نمی دانند و تنها آنها را به صورت فیزیکی نتقل می کنند.

فهوم لایه فیزیکی:

مانی که داده ها از لایه های بالاتر به این لایه می رسند،تنها کاری که بر روی آنها صورت می گیرد این است که به یگنال های الکترونیکی تبدیل می شوند تا از طریق رسانه قابل انتقال شوند. این فرآیند را رمز نگاری سیگنالها Signal Encoding) یا به بیان ساده تر کدگزاری (Encoding) می گویند.

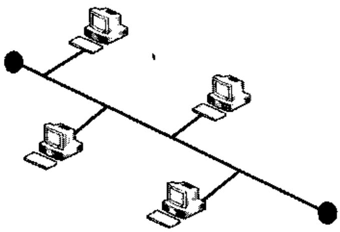
مچنین در این لایه مشخص می شود که چقدر از ظرفیت رسانه فیزیکی برای انتقال داده ها مورد نیاز است . اگر رای ارسال تمامی ظرفیت رسانه مورد استفاده قرار گیرد این نوع انتقال را (Base Band) می گویند.شبکه های حلی مانند اترنت نمونه ای از این نوع هستند.

هرگاه از بخشی از ظرفیت رسانه (فرکانس خاصی) برای انتقال مورد استفاده قرار گیرد به آن (Broad Band) می گویند. سیگنال های تلویزیونی از این نوع هستند.

علاوه بر این ساختار فیزیکی شبکه هم در این لایه تعیین می شود که این امر با کمک توپولوژی ها مشخص می شود. همانگونه که در قبل آموختید توپولوژی نحوه قرار گرفتن رسانه فیزیکی و اتصال آن به اجزاء شبکه است. وپولوژی ها یا فیزیکی یا منطقی و یا تلفیقی از هر دو هستند.

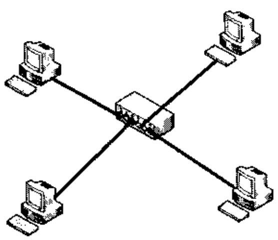
وپولوژی های فیزیکی:خطی (BUS)، ستاره ای (Star)،دایره ای (Ring) و شبکه ای (Mesh) می باشند. که در صل قبلی با همه این توپولوژی ها آشنا شدید. حال تنها جهت یاد آوری مختصری از خصوصیات آنها را ذکر می ماییم.

خطی (BUS):



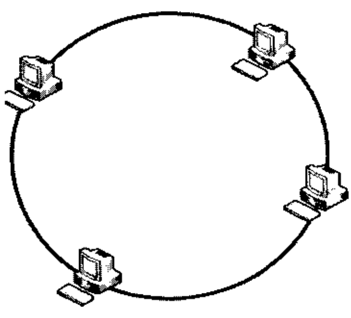
مزیت آن ساده بودن راه اندازی و ارزان بودن می باشد.عیب آن این است که با قطع یک سیستم کل سیستم دچار قطعی می شود.

ستاره ای (Star):



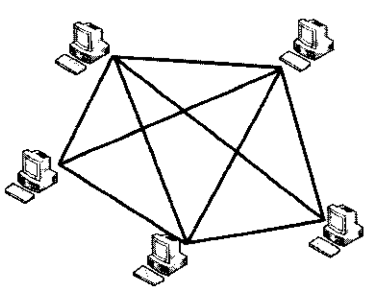
هر سیستم بوسیله یک کابل مجزا به نقطه مرکزی متصل می شود.هزینه راه اندازی گران می باشد اما راه اندازی آن ساده است و در صورت بروز اختلال در یک سیستم ،تنها همان سیستم از شبکه خارج می شود.

دایره ای (Ring):



این نوع توپولوژی به ندرت در شبکه های کامپیوتری دیده می شود.اگر هم بکار گرفته شود در شبکه های گسترده است.به دلیل برخی معایب آن (مشکل بودن راه اندازی،قطع شدن شبکه در صورت قطعی یک سیستم)کمتر از این توپولوژی به صورت فیزیکی استفاده می شود بلکه آن را به صورت تلفیقی از فیزیکی و منطقی بکار می برند مانند : Token Ring که ظاهر فیزیکی آن ستاره ای و از نظر منطقی دایره ای می باشد.در مورد شبکه های Token Ring در بخش بعدی سخن خواهیم گفت.

شبکه ای (Mesh):



این ساختار در شبکه های گسترده آن هم به ندرت مورد استفاده قرار می گیرد. در این ساختارارتباط هر سیستم با دیگر اجزا شبکه از بیش از یک مسیر برقرار شده است.یکی از معایب آن گران بودن ،دشواری راه اندازی و مدیریت آن است. محاسن آن هم در صورت بروز اشکال در یک مسیر،امکان تبادل اطلاعات از مسیر های دیگر وجود دارد.

تجهیزات لایه فیزیکی

بسیاری از تجهیزات که برای هدایت فیزیکی جریان ودر نتیجه داده ها استفاده می شوند در این لایه طبقه بندی می شوند که برخی از آنها به شرح زیر هستند:

- کارت شبکه (NIC)
- تبدیل کننده رسانه (Transceiver)
- تکرار کننده (Repeater)
- هاب (Hub)
- MAU

کارت شبکه (NIC):

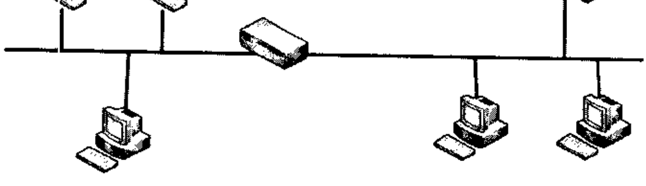
وظیفه برقراری ارتباط فیزیکی با شبکه را برعهده دارد. نوع اتصال موجود در کارت شبکه ،بستگی به نوع پروتکل و ساختار شبکه دارد که می تواند اتصالBNC یا RJ-45 باشد.

تبدیل کننده رسانه (Transceiver):

وسیله ای است که کاربرد اصلی آن برای اتصال کارت شبکه و یاهر دستگاه دیگری به رسانه ای که برای آن ساخته نشده است به عنوان مثال اتصال یک کامپیوتر با اتصال اترنت به شبکه فیبر نوری را می توان نام برد.

تکرار کننده (Repeater):

وسیله ای است که همانگونه که از اسم آن مشخص است برای تکرارو تقویت سیگنال در شبکه استفاده می شود. وزمانی مورد استفاده قرار می گیرد که برخی از اجزا شبکه در فاصله دورتری از دیگر اجزا شبکه قرار داشته باشند.

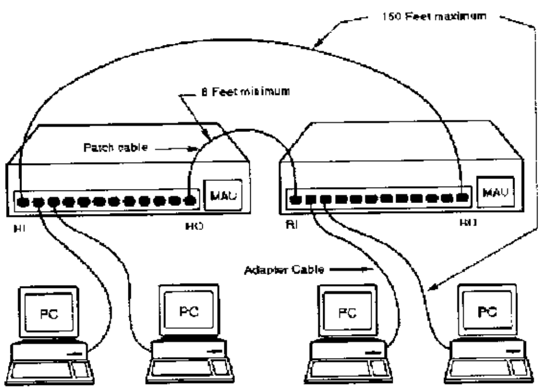


هاب (Hub):

در توپولوژی ستاره ای همه سیستم ها بوسیله کابل های مجزا به نقطه مرکزی که همان هاب است متصل می شوند. HUB وظیفه اتصال اجزا به هم را بر عهده دارد.

MAU(Multistation Access Unit) :

دستگاهی است که تنها در شبکه های Token Ring مورد استفاده قرار می گیرد. همانگونه که گفته شد این شبکه ها ساختار فیزیکی ستاره ای دارند،MAU همانند هاب در شبکه های ستاره ای است.که عملکرد آنها هم بسیار متفاوت با هم است،در هاب داده ها مستقیم برای گیرنده ارسال می شود اما در MAU داده ها در چرخه قرار می گیرند تا گیرنده آن مشخص شود. و محدودیتی هم دارند که می توان حداکثر ۳۳ MAU را به هم متصل نمود .در تصویر زیر شما باساختار فیزیکی این شبکه آشنا می شوید.



لایه دوم : Data Link

این لایه از دو زیر لایه تشکیل شده است:

- MAC (Media Access Control)
- LLC (Logical Link Control)

این بخش از یک سری مطالب مستقل از هم تشکیل شده که تنها اشتراک آنها عملکرد در لایه دوم است.تمام این مطالب به منزله قطعات یک پازل هستند که با کنار هم قرار دادن آنها بنحوه عملکرد این لایه آشنا می شوید.

بحث اصلی در این لایه پروتکل های منطقی و چگونگی ارسال و دریافت داده ها می باشد.

بسته یا Frame :

داده هایی که از لایه های فوقانی به این لایه می رسند،به بسته های کوچکی تقسیم می شوند که به آنها Frame می گویند.در واقع فریم ها کوچکترین و واحد داده های ارتباطی هستند.اندازه و شکل فریم بستگی مستقیم به تکنولوژی ارتباطی دارد.به بیان دیگر فریم ها در دو شبکه اترنت و Token Ringهردو فریم هستند ولی باهم تفاوت اساسی دارند.

پروتکل واحد داده ها PDU (Protocol Data Unit):

ساختار بسته ها یا PDU در هر لایه با هم تفاوت دارد.مثلا در لایه دوم ساختار بسته ها فریم است.در جدول زیر شما با انواع دیگر این ساختار آشنا می شوید:

لایه	ساختار PDU
هفتم (Application)	Message,Datagram,User data
چهارم (Transport)	Segment
سوم (Network)	Packet
دوم (Data Link)	Frame
اول (Physical)	Bits

آدرس فیزیکی سخت افزار ها یا MAC (Media Access Control) :

هر دستگاهی که در شبکه مشغول تبادل اطلاعات است دارای یک آدرس فیزیکی منحصر به فرد است که توسط شرکت سازنده به آن نسبت داده شده است.

این آدرس فیزیکی از ۴۸ بیت ساخته شده است،که معمولاً دارای ۱۲ رقم بر مبنای ۱۶ است که در آن از رقم های ۰ تا ۹ و حروف Aتا F استفاده شده است که هر دو رقم را " : " از هم جدا می کند. به عنوان مثال :

07:57:AC:1F:B2:76

سه بخش اول آدرس (07:57:AC) بیان کننده شناسه شرکت سازنده این دستگاه می باشد و سه بخش دیگر بیان کننده آدرس منحصر بفرد دستگاه مورد نظر است.

این اعداد قابل تغییر نبوده و توسط شرکت سازنده در حافظه فقط خواندنی (ROM) روی دستگاه تعبیه می شود.

توپولوژی های منطقی :

همانطور که قبلاً ذکر شد، توپولوژی فیزیکی چگونگی اتصال را بیان می کرد حال آنکه توپولوژی منطقی چگونگی حرکت داده ها در شبکه را مشخص می کنند. مانند شبکه ای که ازنظر فیزیکی ستاره ای و از نظر منطقی دایره ای است (Physical Star/ Logical ring)

بطور کلی در لایه دوم شبکه ها با توجه به چگونگی دسترسی به اجزا شبکه به ۳ بخش تقسیم می شوند :

- Connection
- Polling
- Tokenpassing

اتصال یا Connection :

در این حالت تمامی اجزاء شبکه به هم متصل هستند و در این صورت می توانند تبادل اطلاعات نمایند.هر سیستم شانس برابر برای ارسال یا دریافت داده ها دارد.

سیستم نوبتی یا Polling :

در این حالت سیستم مرکزی وظیفه کنترل همه سیستم ها را بر عهده دارد. همه سیستم ها با توجه به اولویت در نوبت قرار گرفته تا تبادل اطلاعات بصورت منظم انجام شود و از بوجود آمدن پدیده Collision یا همان تصادف داده ها جلوگیری می شود.

انتقال توکن یا Tokenpassing :

در این سیستم بسته های داده در پوششی به نام Token قرار می گیرند. Token توسط اولین سیستم شبکه ساخته شده و وارد چرخه شبکه می شود.هر سیستمی که این بسته را دریافت کرد می تواند داده های خود را به آن اضافه کرده و ارسال نماید. تنها سیستمی می تواند ارسال اطلاعات کند که این بسته را داشته باشد.این کار از بروز تصادف بین داده ها جلوگیری می کند.

راههای دسترسی به رسانه های شبکه : (Media Access Method)

در شبکه ای که از تعدادی کامپیوتر تشکیل شده است،هر سیستم برای ارسال و دریافت داده ها با دیگران رقابت می کند. برای ایجاد نظم ، ۳ نوع دسترسی به شبکه تعریف شده است:

شناسایی تداخل : CSMA/CD (Carrier Sence Multiple Access/Collision Detection) :

این تکنولوژی امروزه معمولترین تکنولوژی دسترسی است. هرگاه پروتکلی که از این تکنولوژی استفاده می کند بخواهد داه ای را ارسال کند،ابتدا دقت می کند که آیا درون سیم سیگنالی وجود دارد که نشان دهنده انتقال داده باشد، یاخیر،این بخش به عهده بخش (Carrier Sence) است.در صورت عدم وجود سیگنال اجازه ارسال داده را می دهد. سپس بررسی می کند که آیا کاربر دیگری هم در زمان انتقال اقدام به ارسال داده ای می کند؟ اگر ارسال نماید پدیده Collision اتفاق می افتد این بخش کار برعهده بخش شناسایی تداخل (Collision Detection) می باشد.سپس هردو ارسال را برای مدتی معین قطع نموده و مراحل فوق مجدد تکرار می شود تا امکان ارسال داده ها بوجود آید.

Token passing:

در این تکنولوژی همانگونه که قبلا ذکر شد،داده ها در بسته هایی با نام Token منتقل می شوند. Token توسط سیستمی تولید می شود و در چرخه شبکه قرار می گیرد. تنها سیستمی می توان ارسال اطلاعات نماید که Token داشته باشد. با توجه به این توضیحات پدیده تصادف بین داده ها هیچگاه رخ نمی دهد.

جلوگیری از تداخل :CSMA/CA (Carrier Sence Multiple Access/Collision Avoidance) :

در این ساختار بخش اول که وظیفه اش تشخیص داده ها است (Carrier Sence) با تکنولوژی شناسایی تداخل مشابه است. تفاوت در بخش دوم است،در این تکنولوژی به جای ارسال همه داده ،آن را به بخش های کوچکتر (Chunk) تقسیم می کند و یکی از آنها را ارسال می کند.در صورت ارسال صحیح و بدون اشکال ، بسته های دیگر را تا آخرین بسته ارسال می کند. پروتکل Apple Talk از این تکنولوژی استفاده می کند.

پروژه 802 :

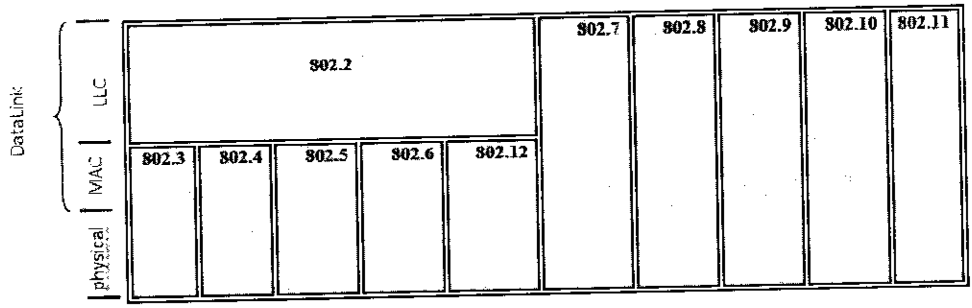
کمیته ای در موسسه بین المللی استاندارد وجود دارد که وظیفه برقراری استاندارد های مختلف برای شبکه های محلی و شهری را برعهده دارد.این کمیته استاندارد را در ماه دوم سال ۱۹۸۰ میلادی وضع نمود و نام آن را به این دلیل نهادند.

در حال حاضر ۱۲ استاندارد زیر مجموعه این پروژه هستند که در جدول صفحه بعدی آنها را مشاهده می نمایید:

استاندارد	موضوع
802.1	LAN/MAN Management
802.2	LLC(Logical Link Control)
802.3	CSMA/CD
802.4	Token Bus
802.5	Token Ring
802.6	DQDB for MAN
802.7	Broadband Local Area Network
802.8	Fiber-Optic LAN and MAN
802.9	Isochronous LANs
802.10	LAN /MAN Security
802.11	Wireless LAN
802.12	Demand Priority Access Method
802.15	Wireless Personal Area Network (WPAN)
802.16	Wireless Metroplitan Area Network(WMAN)
802.17	Resilient Packet Ring
802.18	LAN/MAN Standard Committee

گاهی در کنار برخی از این استاندارد ها حروفی مشاهده می نمایید که مربوط به زیر شاخه و یا برخی نسخه های خاص از آن استاندارد است و استاندارد جدیدی نمی باشند.

نمودار زیر دامنه استفاده و ارتباط استاندارد ها را با مدل OSI نشان می دهد.



استاندارد 802.1 :

در این مبحث استاندارد های شبکه های محلی و شبکه های شهری و مدیریت آنها مورد بحث قرار می گیرد. همچنین تکنولوژی دیگری در این استاندارد در مورد آن بحث می شود Spannig tree است که جهت جلوگیری از تکرار داده ها در شبکه هایی که دارای چندین سوئیچ هستند ، به کار می رود.

استاندارد 802.2 :

این استاندارد در لایه دوم مدل عمل می نماید که وظیفه کنترل منطقی خط (LLC(Logical Link Control را برعهده دارد.در واقع تکنولوژی LLC برقرار کننده ارتباط میان لایه دوم و سوم است.

استاندارد 802.3 :

این استاندارد در مورد شبکه هایی که از پروتکل خطی و سیستم کد کذاری سیگنال Basebandو تکنولوژی ارتباطی CSMA/CD استفاده می نمایند کاربرد دارد.در اکثر منابع این شبکه را اترنت(Ethernet) می نامند.که امروزه پرطرفدار ترین و معمولترین نوع شبکه به دلیل سهولت اجرا و کم هزینه بودن آن است. ساختار جدید این شبکه، با سرعتی بالاتر از استاندارد یعنی GB گیگابیت در ثانیه امروز ه مورد استفاده قرار می گیرد.

استاندارد 802.5 :

این استاندارد درمورد شبکه های Token Ring است.همانگونه که با مشخصات این شبکه آشنا شدید سرعت این شبکه ها در مقایسه با اترنت بسیار پایین تر می باشد،هزینه اجرای آن بالا بوده و در مقابل بروز مشکلات مقاومت اندکی دارد از این رو هیچگاه محبوبیت شبکه های اترنت را پیدا نکرد. امروزه به شکل محدود و آن هم در ابرکامپیوتر های (Main Frame) شرکت IBM استفاده می گردد.

استاندارد 802.10 :

این استاندارد ابتدا برای ایجاد امنیت در شبکه های محلی شهری جهت تامین امنیت داده های اشتراکی در این شبکه ها به کار می رفت. مکانیزم عمل به این صورت است که برای ایجاد امنیت ،شبکه های محلی مجازی VLAN(Virtual Local Area Network) درون شبکه اصلی ایجاد می شود که تنها کامپیوتر هایی که عضو این شبکه مجازی هستند اجازه تبادل داده با هم را دارا هستند وهیچ کامپیوتری خارج از این شبکه مجازی اجازه ورود و اشتراک اطلاعات با کاربران درون شبکه را ندارد.

برای کنترل دسترسی ها به این شبکه از مکانیزم کنترل دسترسی (Authentication) استفاده می گردد تا اطمینان حاصل گردد هیچ سیستمی بدون مجوز وارد این محیط نگردد.

استاندارد 802.11 :

این استاندارد مربوط به شبکه های بدون سیم است. اگرچه استفاده از این تکنولوژی در مقایسه با شبکه های اترنت بسیار کمتر است وهزینه تجهیزات آن گرانتر از شبکه های معمول است اما در پاره ای اوقات با توجه به شرایط بسیار مقرون به صرفه تر است.

هرگاه نیاز به ایجاد شبکه ای در زمانی کوتاه باشد قطعاً انتخاب شما شبکه بدون سیم است.زیرا شما می توانید در فاصله مجاز از این تجهیزات حرکت نموده و به راحتی کل این شبکه را از جایی به جای دیگر منتقل نمایید. فرض نمایید پس از بروز حادثه ای طبیعی هلال احمر یا صلیب سرخ بخواهند پایگاهی ایجاد نموده و پس از چند ساعت و یا چند روز به راحتی آن را جمع آوری نمایند. در این نوع موارد از شبکه های بدون سیم استفاده می شود.

امروزه زیر شاخه های جدیدی از این استاندارد بوجود آمده(802.11a,b,g) که توانایی انتقال داده ها حتی تا چندین برابر استاندارد اولیه(802.11g 54 mbps) که انتقال بین ۱ تا ۲ مگابیت بر ثانیه را دارا هستند. البته با دیگر خصوصیات این شبکه در فصل های بعدی آشنا خواهید شد.

استاندارد 802.12 :

این استاندارد ابتدا توسط شرکت HP (Hewlet-Packard) بنا نهاده شد و هدف آن تلفیق توانایی های شبکه های اترنت(Ethernet) وتوکن رینگ(Token Ring) با هم بود.در این استاندارد از هاب های هوشمند استفاده می شود که می توانند اولویت بندی نموده و پهنای باند بیشتری را به سیستم های دارای اولویت بالا تر اختصاص دهند.این استاندارد با نام های: 100VG(Voice Grade)، 100VG-AnyLAN، 100Base-VG وAnyLAN هم مشهور هستند.

در جدول زیر خلاصه مشخصات چند تکنولوژی معروف و پر استفاده را مشاهده می نمایید:

تکنولوژی	سرعت تبادل داده ها	تکنولوژی دسترسی	توپولوژی	رسانه فیزیکی
IEEE 802.3	10,100,1000,10000 Mbps	CSMA/CD	Logical BUS	Coax or UTP
IEEE 802.5	4,16,100 Mbps	Token Passing	Physical STAR / Logical RING	STP or UTP
IEEE 802.11	1,11,54 Mbps	CSMA/CA	Cellular	RF through Air
FDDI	100 Mbps	Token Passing	Physical STAR / Logical RING	Fiber Optic

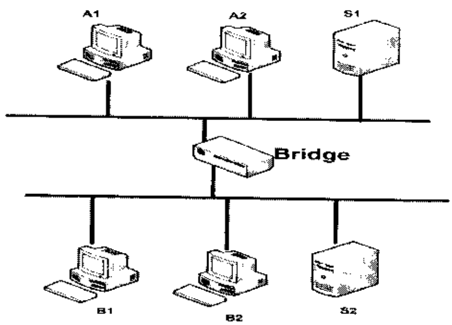
تجهیزات لایه دوم :

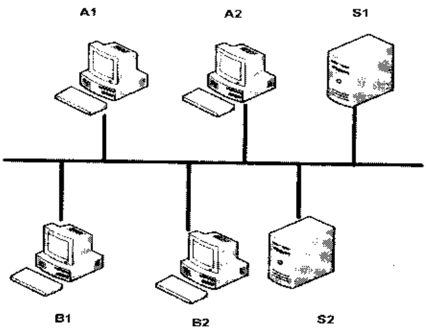
در این لایه تجهیزات زیر مورد استفاده قرار می گیرد:

- پل ارتباطی Bridge
- سوئیچ Switch
- نقطه دسترسی بیسیم WAP

پل ارتباطی Bridge:

این دستگاه برای اتصال دو شبکه همسان به یکدیگر و یا برای تقسیم بار وترافیک شبکه استفاده می شود. در این حالت، حدود ۲۰٪ از ترافیک شبکه از پل ارتباطی عبور می نماید.



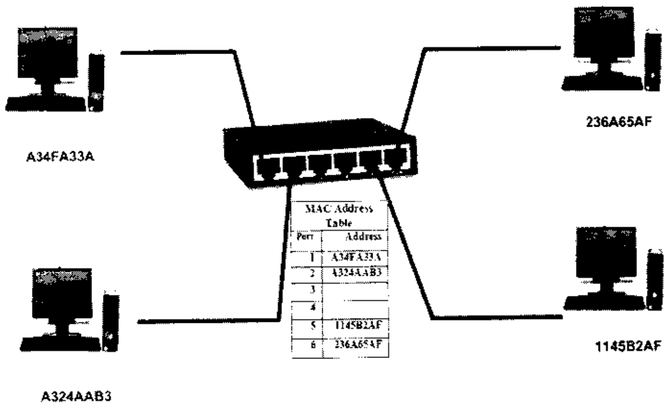


سوئیچ Switch :

دستگاه مرکزی که همانند هاب وظیفه اتصال اجزاء شبکه به هم را برعهده دارد،البته بسیار هوشمند تر از هاب است. در این بخش منظور از سوئیچ ،سوئیچ لایه دوم است.

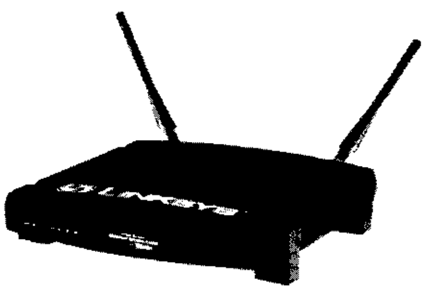
این دستگاه جدولی از تمامی آدرس های فیزیکی (MAC)تجهیزات شبکه را تهیه می نماید،حال هرگاه دو سیستم بخواهند تبادل اطلاعات داشته باشند، آدرس گیرنده را از داده استخراج نموده و پس از تطبیق با جدول آدرس ها ؛ داده را مستقیم برای گیرنده ارسال می نماید.

البته نوع دیگری سوئیچ هم در لایه سوم قرار دارد که علاوه بر این کار قابلیت مسیریابی هم دارد که در جای خود به آن می پردازیم.



نقطه دسترسی بیسیم یا WAP:

نقطه دسترسی بیسیم WAP (Wireless Access Point) وسیله است که برای اتصال تعدادی کامپیوتر در شبکه بدون سیم و برقراری اتصال آنها با یک شبکه سیمی عمل می نماید.می توان گفت این دستگاه معادل بدون سیم سوئیچ است.



این دستگاه حداقل دارای یک آنتن است که برای تقویت دریافت سیگنال ها بکار می رود.علاوه بر این وظیفه می توان از این دستگاه برای اتصال دوشبکه بدون سیم به عنوان یک پل ارتباطی هم استفاده نمود.

لایه های میانی مدل OSI

هرچه در این مدل از پایین به سمت بالا حرکت نماییم،پروتکل ها پیچیده تر و وظایف آنها هم بیشتر و مهم تر می شود. در این بخش دو لایه سوم و چهارم را مورد بحث قرار می دهیم.

لایه سوم (Network Layer) :

در این لایه باستفاده از پروتکل های لایه شبکه کمک می کنند تا داده ها به مقصد صحیح خود برسند.این لایه مهمترین لایه در مدل است که در خصوص آن بسیار سخن خواهیم گفت.

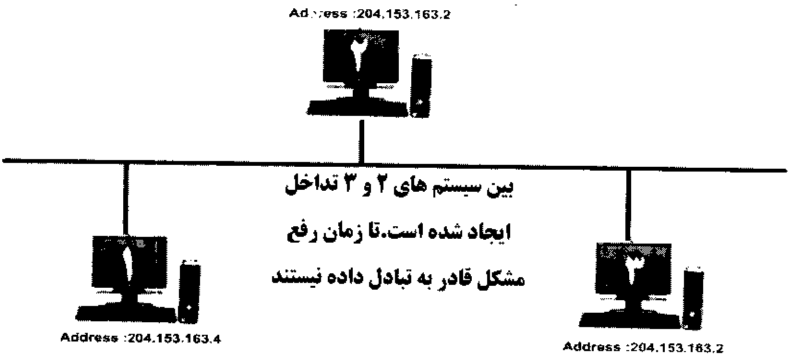
در این لایه ۲ عمل مهم انجام می گیرد : ارایه آدرس منطقی و مسیریابی که در خصوص هرکدام به تفصیل سخن خواهیم گفت.

آدرس دهی منطقی (Logical Network Adressing):

در گذشته آموختید که هرسیستمی در شبکه برای تبادل داده ها نیاز به یک آدرس فیزیکی منحصر بفرد می باشد که توسط شرکت سازنده در آن تعبیه شده است وقابل تغییر نبوده و همچنین مستقل از پروتکل می باشد.

اما بسیاری از شبکه ها از پروتکل خاصی استفاده می نمایند که نیازمند آدرس های خاصی است که مطابق با پروتکل تعریف شده باشد.

آدرس منطقی شبکه ،کاملاً وابسته به پروتکل بوده و شکل و فرمت آن در هرپروتکل متفاوت است.لازم به ذکر است هیچ دو کامپیوتری در شبکه نباید آدرس منطقی یکسان داشته باشند.هرگاه ۲ سیستم آدرس یکسان داشته باشند پدیده تداخل (Conflict) اتفاق افتاده و تا زمان رفع این مشکل قادر به تبادل اطلاعات در شبکه نمی باشند.



فرمت های آدرس:

قبل از این که شما شبکه ای را راه اندازی کنید و یا بخواهید دستگاهی را به شبکه اضافه نمایید،می بایست شکل صحیح آدرس در شبکه را بشناسید.

صرفنظر از پروتکل، چهTCP/IP باشد و یاIPX ،هر آدرس از دو بخش تشکیل شده است: بخش شبکه و بخش میزبان

بخش شبکه مربوط به قسمت خاصی از شبکه است که کامپیوتر در آن قرار دارد.بخش میزبان ،آدرس منحصر بفردی است که سیستم خاصی را در بخش شبکه مشخص می نماید. مجموع دو بخش شبکه ومیزبان در آدرس می بایست در شبکه منحصر بفرد باشد تا نمایشگر سیستم خاصی در شبکه باشد.

آدرس های پروتکلIPX از ۳۲ بیت تشکیل شده اند.بخش شبکه از ۸ رقم در مبنای ۱۶ تشکیل شده و بخش میزبان ۱۲ رقم در مبنای ۱۶ است که همان آدرس فیزیکی (MAC) دستگاه است.

00004567:006AC11FB56

بخش شبکه بخش میزبان

در سوی دیگر ، در پروتکلTCP شکل آدرس دهی متفاوت است.آدرس ها از ۳۲ بیت تشکیل شده که بین هربخش با نقطه از هم جدا می شود. که با شکل کلی زیر است:

XXX.XXX.XXX.XXX

که در این حالت X می تواند رقمی بین ۰ تا ۹ باشد و XXX عددی بین ۰ تا ۲۵۵ باشد. این آدرس که به IP Address مشهور است که امروزه معمولترین نوع آدرس دهی است.

ذکر این نکته ضروری است که پدیده تداخل یا Conflict تنها مربوط به شبکه های TCP است .زیرا در پروتکل IPX آدرس ها هیچگاه نمی توانند یکسان باشند.و دلیل آن هم استفاده از آدرس فیزیکی تجهیزات است.

بسته یا Packet:

در لایه سوم،داده هایی که از لایه های بالاتر به این لایه می رسند بصورت منطقی به بخش های کوچکتری با نام Packet یا بسته تقسیم می شوند. اندازه و ساختار آنها بستگی مستقیم به پروتکل شبکه دارد .به بیان دیگر Packet در TCP با Packet در IPX بسیار متفاوت است.

مسیریابی یا Routing :

پروسه ای که در آن داده ها از داخل شبکه و از بین بخش های مختف آن عبور نموده تا به مقصد نهایی خود برسد را مسیر یابی یا Routing می گویند.

اینتر نتورک یا درون شبکه:

هرگاه یک شبکه توسط روتر یا همان مسیریاب به چند بخش تقسیم شود هرکدام را یک زیر شبکه یاInternetwork می گویند.

مسیریاب ها انتخاب بهترین مسیر را با کمک بانک اطلاعاتی درون خود که به صورت یک جدول از مشخصات سیستم های مختلف است،انجام می دهند. این جدول ممکن است به صورت دستی (Static) و یا به صورت خودکار (Dynamic) تهیه شده باشد.

در مسیریابی خودکار،مسیریاب ها با دیگر مسیریاب های متصل به شبکه تعامل داشته و مشخص می نمایند که هرکدام به چه شبکه ای متصل هستند. وطی زمان خاصی اطلاعات و همچنین اتصال خود را به روز می نمایند.

پروتکل های مسیریابی بطور کلی بر ۲ نوع می باشند: بر اساس مسافت یا distance vector وبر اساس وضعیت خط ارتباطی یا link state

distance vector : این پروتکل ها شبکه های همسایه را شناسایی کرده و طی الگوریتم خاصی بهترین مسیر را انتخاب نمایند.ضمنا در طی زمان های خاصی اطلاعات خود از شبکه های همسایه را به روز می نمایند.در این پروتکل ملاک انتخاب مسیر کوتاه تر است. پروتکل RIP از این دسته است.

link state : این پروتکل ها بسیار به صرفه تر هستندزیرا مسیریاب ها تنها در صورت لزوم اطلاعات خود را به روز می نماید از این رو بار کمتری بر مسیریاب تحمیل می شود و پهنای باند کمتری مورد استفاده قرار می گیرد. وضعیت خط ارتباطی ملاک اصلی برای انتخاب مسیر مورد نظر است .پروتکل OSPF از این دسته است.

البته باید به یاد داشت که تمامی پروتکل ها قابلیت مسیریابی ندارند.شما می بایست با پروتکل هایی که این قابلیت را دارا هستند آشنا شوید.جدول زیر به شما کمک خواهد کرد با این پروتکل ها آشنا شوید.

پروتکل	پروتکل مسیر یابی	آیا قابل مسیریابی است؟
IPX	RIP	بله
IPX	NLSP	بله
NetBEUI	ندارد	خیر
TCP/IP	RIP	بله
TCP/IP	OSPF	بله
XNS	RIP	بله



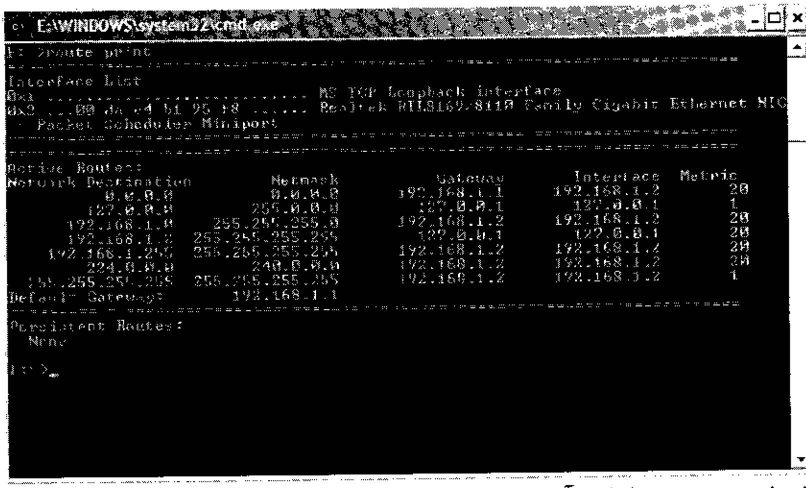
هرگاه شما مسیریابی را در شبکه فعال می نمایید، می بایست دروازه خروجی پیش فرض یا (Default Gateway) شبکه را هم معین نمایید.این دروازه خروجی می تواند بخشی از مسیریاب باشد از یک سو با اجزا شبکه هم آدرس است و به شبکه متصل است و از سوی دیگر به شبکه دیگری متصل است و می تواند داده های را از شبکه به شبکه ای دیگر منتقل نماید.

اگر شمامسیریاب را به عنوان دروازه خروجی پیکر بندی نمایید،سیستم های شبکه می بایست آدرس مسیر یاب را به عنوان درگاه خروجی خود مشخص نمایند. در این بخش چگونگی اضافه کردن دروازه خروجی به سیستم های ویندوز و مسیریاب های سیسکو را خواهید آموخت.

❖ الف:سیستم های مبتنی بر سیستم عامل ویندوز :

در منوی آغاز گزینه اجرا(RUN) را انتخاب نموده و فرمان CMD را تایپ و سپس فرمان Route Print را نوشته و آن را اجرا می نمایید.

در تصویر زیر خروجی این پروسه را مشاهده می نمایید:



دروازه خروجی سیستم شما در آخرین خط مشخص شده است

Default Gateway : 192.168.1.1

برای افزودن یک دروازه خروجی از فرمان زیر استفاده می شود:

Route add xxx.xxx.xxx.xxx mask xxx.xxx.xxx.xxx

برای حذف کردن یک درگاه خروجی از لیست فرمان از دستور زیر استفاده می شود:

Route delete xxx.xxx.xxx.xxx mask xxx.xxx.xxx.xxx

❖ ب:در تجهیزات سیسکو :

در این تجهیزات سیستم عامل (Cisco IOS) جدول بسیار پیشرفته تری نسبت به ویندوز تهیه می کند و پروسه پیشرفته تری برای مسیریابی اجرا می شود. ذکر این نکته ضروری است که مسیریابها معمولاً دارای چندین پورت هستند که هرکدام می توانند به عنوان دروازه خروجی استفاده شوند که ذکر نوع پورت و شماره آن ضروری است. همچنین

کار با این تجهیزات نیاز به آشنایی با تکنولوژی سیسکو دارد که از حوصله این بحث خارج است،تنها برای آشنایی این بخش را مشاهده می نمایید.

برای نمایش جدول مسیریابی دستور زیر را اجرا می نماییم :

Router# Show ip route

تصویر زیر خروجی فرمان **Show ip route** را نمایش می دهد:

```
Router_1700#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 5 subnets
C       172.16.4.0 is directly connected, Serial0
C       172.16.5.0 is directly connected, Serial1
R       172.16.1.0 [120/3] via 172.16.4.1, 00:00:22, Serial0
R       172.16.2.0 [120/2] via 172.16.4.1, 00:00:22, Serial0
R       172.16.3.0 [120/1] via 172.16.4.1, 00:00:22, Serial0
R    192.168.4.0/24 [120/2] via 172.16.4.1, 00:00:22, Serial0
R    192.168.5.0/24 [120/1] via 172.16.4.1, 00:00:22, Serial0
C    192.168.6.0/24 is directly connected, FastEthernet0
R    192.168.7.0/24 [120/1] via 172.16.5.2, 00:00:12, Serial1
R    192.168.1.0/24 [120/4] via 172.16.4.1, 00:00:24, Serial0
R    192.168.2.0/24 [120/3] via 172.16.4.1, 00:00:24, Serial0
R    192.168.3.0/24 [120/2] via 172.16.4.1, 00:00:09, Serial0
```

برای تغییر در جدول و اضافه کردن یک مسیر و دروازه خروجی از دستورات زیر استفاده می شود:

Router# configure terminal

Router(config)#ip route 0.0.0.0 0.0.0.0 serial 0

Router(config)# end

Router#

در فرمان های فوق ، دروازه خروجی پورت سریال 0 مسیریاب است.

برای حذف این مسیر تعریف شده ، مراحل زیر را انجام می دهیم :

Router# configure terminal

Router(config)#no ip route 0.0.0.0 0.0.0.0 serial 0

Router(config)# end

Router#

حال که با مسیریابی و تغییر درگاه خروجی در این تجهیزات آشنا شدیم به سراغ معرفی تجهیزات لایه سوم می رویم.

تجهیزات لایه سوم :

تجهیزات این لایه مهمترین وپیچیده ترین و در عین حال گرانترین تجهیزات شبکه هستند.

- مسیریاب Routers
- سوئیچ لایه سوم Layer 3 switch

مسیریاب :

همانگونه که در گذشته بحث شد،وسیله ای بسیار پیچیده که وظیفه مسیریابی و انتخاب بهترین مسیر برای ارسال داده ها را برعهده دارد. می توان گفت که مسیریاب گرانترین و پیچیده ترین دستگاه شبکه است.

سوئیچ لایه سوم :

این دستگاه علاوه بر عملکرد های همتای خود در لایه دوم، می تواند مسیریابی را در سطح محدودی انجام دهد که این قابلیت آن را متمایز از سوئیچ های لایه دوم می نماید.

لایه چهارم

در این لایه انتقال داده هاصورت می گیرد. کنترل خطا های ارتباطی و ایجاد ارتباطی دو سویه هم از وظایف این لایه است. پروتکل های این لایه ارتباطی مطمئن و قابل اعتماد را برای تبادل داده ها ایجاد می کنند. البته هر قانونی استثنایی هم دارد ودر این مورد پروتکل UDP می باشد. که در مورد آن هم سخن خواهیم گفت.

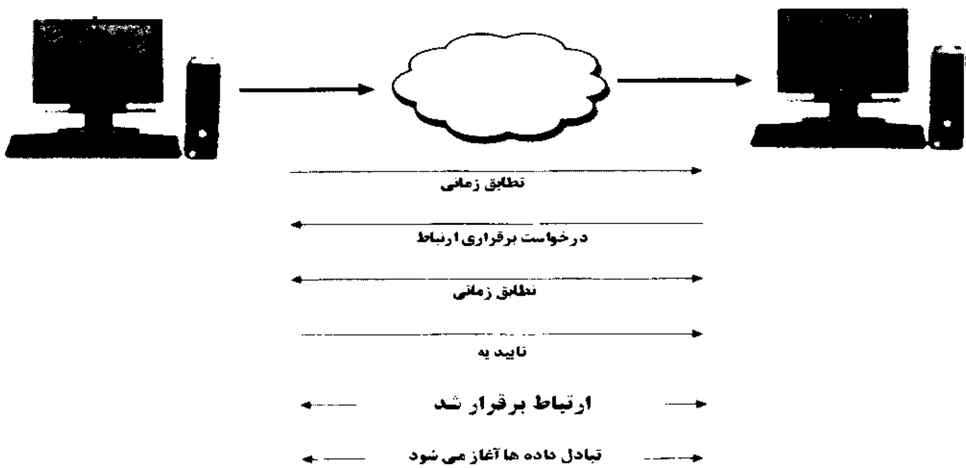
بطور کلی ۲ نوع پروتکل های ارتباطی وجود دارد:

- وابسته به اتصال Connection Oriented
- مستقل از اتصال Connectionless

پروتکل های وابسته به اتصال :

در این پروتکل ها قبل از آغاز ارسال داده می بایست ارتباط برقرار شده باشد و گیرنده آماده دریافت داده ها شده باشد. می توان این ارتباط را با مکالمه تلفنی مشابه دانست.

در تماس تلفنی شما شماره مشترک را می گیرید،گیرنده گوشی را برداشته و مکالمه آغاز می شود.اگر سکوت شما طولانی باشد از شما سوال می کند که هنوز ارتباط برقرار است؟ در زمان پایان مکالمه هم ارتباط از سوی هر دوطرف مکالمه قطع می شود . تصویر مراحل برقراری ارتباط تا ارسال داده ها را نمایش می دهد:



پروتکل های مستقل از اتصال :

این پروتکل ها بر خلاف مبحث قبلی نیاز به مراحل خاصی قبل از ارسال داده ندارند و پس از ارسال هم خطاهای احتمالی را کنترل نمی نمایند. در واقع ارتباط این پروتکل ها قابل اطمینان نیست. تنها یک حسن دارد و آن هم سرعت است. هرکجا که داده ها اهمیت خاصی نداشته باشند و سرعت ارسال اهمیت د اشته باشد(ارسال تصاویر زنده تلویزیونی و رادیویی)،از این پروتکل ها استفاده می شود.

پیش از ادامه مباحث مربوط به لایه چهارم ،به معرفی پروتکل های مورد استفاده در این لایه می پردازیم:

- TCP/IP
- IPX/SPX
- NetBEUI

پروتکل IPX/SPX:

این پروتکل از دو بخش تشکیل شده است:

IPX(Internetwork Packet Exchange)

SPX(Sequenced Packet Exchange)

بخش IPX مستقل از اتصال وSPX وابسته به اتصال است. که هر کدام مستقل می توانند فعالیت نمایند.

پروتکل TCP/IP:

این پروتکل نیز از دو بخش تشکیل شده است:

TCP (Transmission Control Protocol)

UDP (User Datagram Protocol)

TCP وابسته به اتصال و UDP مستقل از اتصال است.برخی از پروتکل های لایه بالاتر مانند (HHTPو FTP)نیازمند اتصالی مطمئن و بدون اشکال هستند واز TCP استفاده می کنند.برخی دیگر تنها مولفه سرعت در آنها مهم است(TFTP) که از UDP استفاده می کنند.

پروتکلNetBEUI :

این پروتکل که برای لایه شبکه طراحی شده است، پشتیبانی از شبکه های مبتنی بر پروتکل NetBIOS را بر عهده دارد. این پروتکل توسط IBM طراحی شده بود و مایکروسافت و ناول آن را توسعه دادند تا برای استفاده در سیستم های عامل شبکه مانند WindowsNTو Windows 2000 قابل استفاده باشند. این پروتکل بسیار سریع بوده و بار کمی را بر شبکه تحمیل می نمود و برای شبکه های کوچک که بین ۱۰ تا ۲۰۰ کاربر داشتند طراحی شده بود.
در این بخش با مولفه های این پروتکل مانند مسیریابی،آدرس دهی و نامگذاری آشنا می شویم.

آدرس دهی و نامگذاری:

در شبکه های امروزی بسیار کم و به ندرت از این پروتکل ها استفاده می نمایند.آدرس و نام در این شبکه ها یکسان است.هر سیستم -دقت نمایید هرسیستم نه هر درگاه-دارای یک نام منحصر بفرد در شبکه است .البته انتخاب نام بسیار مهم است،نام حداکثر می تواند شامل ۱۵ کاراکتر باشد که بسیار ساده و سریع انجام می شود.

مسیریابی :

از آنجاییکه این پروتکل فاقد ساختار واحد نامگذاری و آدرس دهی می باشدقابل مسیریابی نیست و مسیریاب ها بسته های این پروتکل را حذف می نمایند.تنها در موارد خاص می توان مسیریاب را به گونه ای تنظیم نمود که همانند پل ارتباطی این بسته ها را عبور دهد.

قابلیت همکاری:

تنها سیستم عامل های محدودی بسته پروتکل NetBIOS/NetBEUI را پشتیبانی می نمایند.سیستم عامل شرکت اپل – مکینتاش از این پروتکل پشتیبانی نمیکند.البته لازم به ذکر است که سیستم عامل های جدید مایکروسافت هم از این پروتکل پشتیبانی نمیکنند اما یک تفاوت دارند که پشتیبانی این پروتکل را می توان به سیستم عامل های خانواده مایکروسافت اضافه نمود.

Apple Talk/ Apple Talk Over IP

هنگامی که اپل مکینتاش را در سال ۱۹۸۴ معرفی کرد، مک (Mac)دارای نرم افزار شبکه بود، این نرم افزار بر مبنای پروتکل Apple Talk بنا نهاده شده بود و استاندارد کابل کشی شبکه بر اساس Local Talk بود که شبکه ای بسیار پیش پا افتاده و ساده بود.به مرور زمان کاربران خواهان تغییرات و ارایه نسخه جدید بودند که نسخه دوم پروتکل Apple Talk معرفی شد که از شبکه اترنت پشتیبانی می نمود و سرعت و کارایی بالاتری داشت.

آدرس دهی:

هرسیستم در این شبکه از آدرسی که ۲۴ بیت طول دارد استفاده می کند که ۱۶ بیت آن مربوط به شبکه است که قابلیت آدرس دهی به ۲۵۴ کاربر شبکه را دارد.آدرس هر سیستم به صورت خودکار توسط خود همان سیستم تعیین می شود.

قابلیت همکاری:

تنها سیستمی که از ابتدا پروتکل Apple Talk روی آن قرار دارد مکینتاش می باشد.در بسیاری از سیستم عامل های ویندوز در صورت نصب نرم افزار پشتیبانی ،امکان برقراری ارتباط با این سیستم ها را خواهند داشت.

نامگذاری:

Apple Talk برای نامگذاری سیستم ها از پروتکل خاصی به نام NBP (Name Binding Protocol) استفاده می کند.نحوه نامگذاری به این شرح است که هر سیستم در زمان ورود به شبکه نام خود را برای شبکه ارسال می کند.مسیریاب شبکه این نام را ذخیره نموده تا در زمان مورد نیاز تبادل داده ها آن را در دسترس سیستم ها قرار دهد.

جمع بندی:

در این بخش شما:

- با مدلOSI و برخی پروتکل های پرطرفدار و مهم شبکه آشنا شدید.
- در مورد ۷ لایه مدل OSI مطالبی آموختید و با خصوصیات هر لایه به تفکیک آشنا شدید.
- در خصوص پروتکل های شبکه مانند : TCP/IP، NetBEUI/NetBIOS، IPX/SPX و Apple Talk مطالب مفیدی آموختید و با مولفه های اصلی در هرکدام از این پروتکل ها آشنا شدید.
- با استاندارد802 و زیر استاندارد های آن آشنا شدید.

سوالات ارزیابی برای آزمون Network+ :

۱ -در کدامیک از لایه ها ارتباط قابل اعتماد و دو سویه برقرار می شود.

الف) لایه شبکه.
ب) لایه انتقال.
ج) لایه جلسه.
د) لایه نمایش.

۲ -در کدامیک از لایه ها امکان مسیر یابی وجود دارد.
الف) لایه جلسه.
ب) لایه شبکه
ج) لایه شبکه
د) لایه نمایش.

۳ -در کدامیک از لایه ها داده هایی که از لایه های بالایی رسیده اند به سیگنال تبدیل شده و توسط کابل ارتباطی منتقل می شوند .

الف) لایه جلسه.
ب) لایه شبکه
ج) لایه شبکه
د) لایه نمایش.

۴ -در کدام استاندارد در مورد شبکه های بیسیم صحبت می شود.
الف) 802.1
ب) 802.3
ج) 802.5
د) 802.11

۵ –کدامیک از تجهیزات ریسک بوجود آمدن تصادف یا Collisioin را افزایش می دهد.
الف) پل ارتباطی
ب) هاب
ج) سوییچ

د) مسیریاب

۶ –کدام گزینه می تواند آدرس فیزیکی یا MAC باشد .

الف) 199.163.217.45

ب) 00076968731467

ج) 01:A5:BB:A7:FF:60

د) 00:4N:B0:AD:F8:2A

۷ –مسیریاب در کدام لایه فعالیت می نماید.

الف) لایه جلسه.

ب) لایه شبکه

ج) لایه شبکه

د) لایه نمایش.

۸ –کدامیک از تجهیزات زیر می تواند جایگزین هاب برای افزایش کار آیی شبکه شود.

الف) پل ارتباطی

ب) مبدل رسانه

ج) مسیریاب

د) سوییچ

۹ –کدامیک از پروتکل های زیر وابسته به اتصال هستند .

الف) HTTP

ب) TCP

ج) TFTP

د) NetBios

۱۰ – شما به اشتباه بر روی دو سیستم یک آدرس IP تنظیم می نمایید. پیام خطا بر روی کدام سیستم به نمایش در می آید.

الف) سیستم اول

ب) سیستم دوم

ج) پیام خطایی نمایش داده نمی شود.

د) بر روی هر دو سیستم نمایش داده می شود.

پاسخ به سوالات این بخش

۱ -**ب**

بر قراری ارتباط دو سویه وظیفه لایه چهارم است.

۲ -**ب**

در لایه سوم یا همان لایه شبکه امکان مسیریابی داده ها از مبدا به مقصد وجود دارد.

۳ -**ج**

در لایه فیزیکی (Physical) داده ها به سیگنال های الکتریکی تبدیل شده تا از طریق کابل در شبکه منتقل شوند.

۴ -**د**

در استاندارد 802.11 در مورد شبکه های بیسیم صحبت می شود.

۵ -**ب**

استفاده از هاب شانس بروز تصادف یا Collision را افزایش می دهد.
در سوییچ ها با کمک مکانیزم های نظارتی از بروز Collision جلوگیری می شود.

۶ - **ج**

مطابق تعریف آدرس فیزیکی آدرسی است ۶ بخشی که بین هر بخش علامت : وجود دارد. به علاوه این اعداد در مبنای ۱۶ هستند. یعنی ۰-۹ و a تا f
گزینه صحیح ج است

۷ -**ج**

مسیریاب در لایه سوم یا شبکه فعالیت می نماید.

۸ -**ب**

پل ارتباطی برای برقراری ارتباط منطقی بین اجزای شبکه مورد استفاده قرار می گیرد.
مسیریاب برای مسیریابی بین اجزای شبکه بکار می رود.
سوییچ برای برقراری ارتباط فیزیکی بین اجزا شبکه می باشد. که می تواند جایگزین مناسبی برای هاب باشد

۹ -الف ، ب

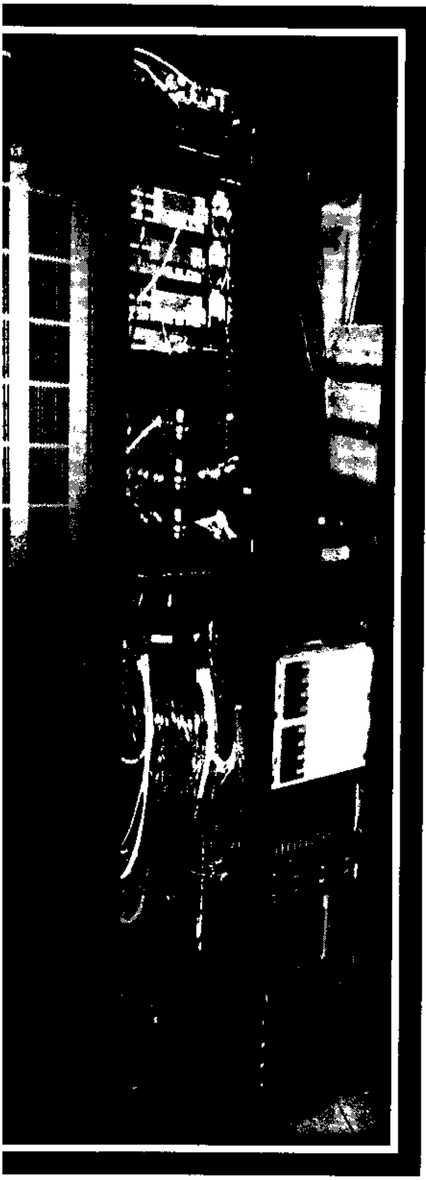
پروتکل TFTPبر اساس پروتکل ارتباطی UDP فعالیت می نماید از این رو مستقل از اتصال است.

۱۰ ج

پیام خطای آدرس تکراری بر روی هر دو سیستم نمایش داده می شود.

فصل سوم

مبانی TCP/IP



شما در این فصل با این مفاهیم آشنا خواهید شد:

۳-۱ شناسایی تفاوت های پروتکل های شبکه از نظر مسیریابی ،آدرس دهی ،ارتباط داخلی ونامگذاری در پروتکل های:

- IPX/SPX
- NetBEUI
- Apple Talk/Apple Talk Over IP
- TCP/IP

۳-۲ شناسایی اجزا و ساختار آدرس IP و تنظیمات مورد نیاز جهت کار در محیط اینترنت

۳-۳ آشنایی با کلاس های IP (class A , B &C)و دامنه هرکدام ازاین کلاس ها و تقسیم بندی زیر شبکه (Subnet Mask) آنها

۳-۴ شناسایی اهداف تقسیم بندی دهی زیر شبکه (Subnet Mask)

۳-۵ شناسایی تفاوت بین IP های عمومی (Public) و خصوصی(Private)

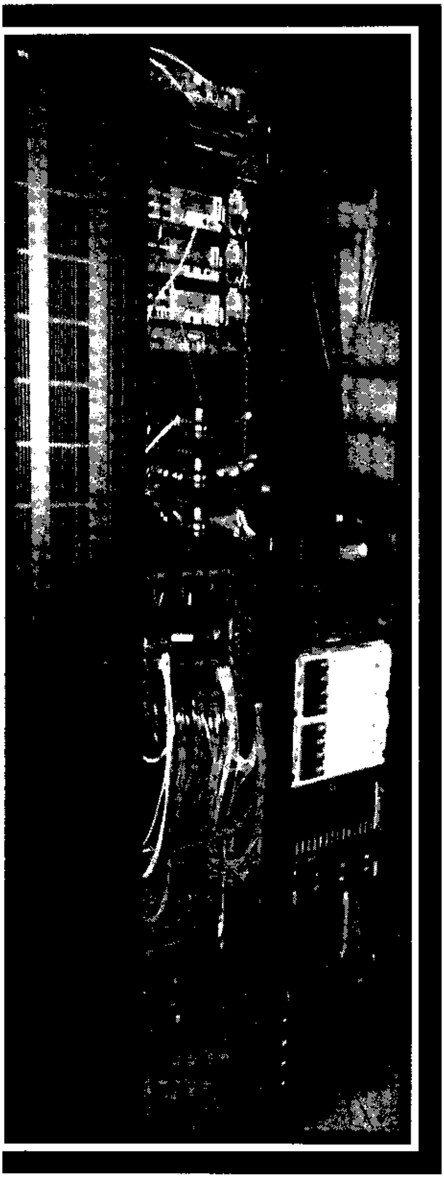
۳-۶ شناسایی تفاوت بین انواع آدرس دهی شبکه:

- ایستا (Static)
- پویا (Dynamic)
- آدرس دهی توسط خود سیستم (Self Addressing - APIPA

۳-۷ تعیین کردن هدف،کارکرد و استفاده از پروتکل های زیر

- (Transmission Control Protocol) TCP
- (User Datagram Protocol) UDP
- (File Transfer protocol) FTP

فصل سوم



- (Secure File Transfer protocol) SFTP
- (Trivial File Transfer protocol)TFTP
- (Simple Mail Transfer protocol)SMTP
- (Hyper Text Transfer protocol)HTTP
- (Hyper Text Transfer protocol Secure)HTTPS
- (POP3/IMAP4Post Office protocol ver3/
- Internet Message Access protocol ver4)
- Telnet
- (Secure Shell) SSH
- (Internet Control Message protocol) ICMP
- Adress Resolution protocol/) ARP/RARP

reverse Adress Resolution protocol)

- (Network Time protocol) NTP
- (Network News Transfer protocol) NNTP
- (Secure Copy protocol) SCP
- (Lightweight Directory Access protocol) LDAP
- (Internet Group Management protocol) IGMP
- (Line Printer Remote) LPR

۳-۸ تعیین کارکرد های هر پورت درپروتکل های TCP/UDP

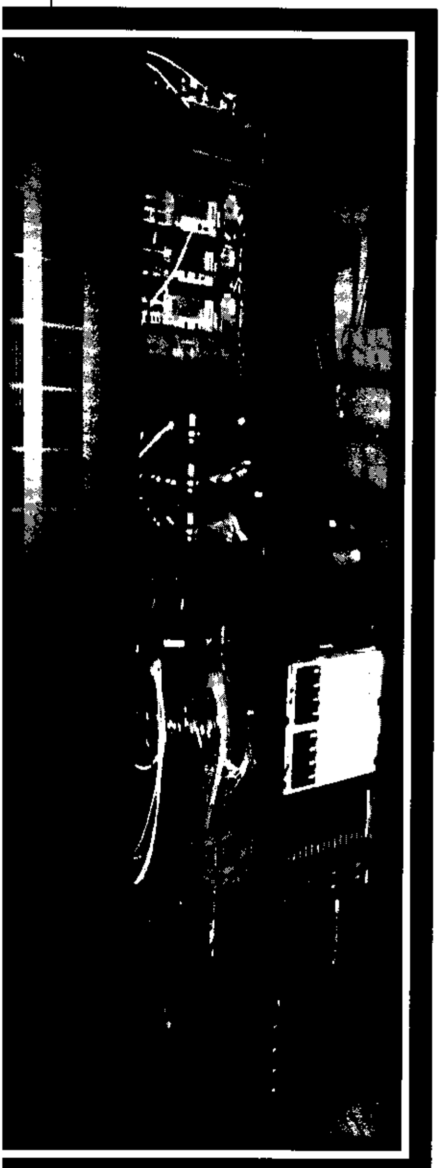
۳-۹ شناسایی شماره پورت های معروف و سرویس های مرتبط با هرکدام

- 20 FTP
- 21 FTP
- 22 SSH
- 23 Telnet
- 25 SMTP
- 53 DNS
- 69 TFTP
- 80 HTTP
- 110 POP3
- 119 NNTP
- 123 NTP
- 143 IMAP4
- 443 HTTPS

۳-۱۰ شناسایی اهداف هر یک از سرویس های شبکه مانند

- (Domain Name System)DNS
- (Network Adress Translation) NAT
- (Internet Connection Sharing) ICS

فصل سوم



- (Windows Internet Naming Service) WINS
- (Simple Network Management Protocol) SNMP
- (Network File System)NFS
- (Zero Configuration)Zeroconf
- (Server Message Block) SMB
- (Apple File Protocol)AFP
- (Line Printer Daemon) LPD

۳-۱۱ شناسایی اهداف ،خصوصیات و مزایای استفاده ازسرویس پروکسی

۳-۱۲ شناسایی خصوصیات شبکه داخلی مجازی VLANs(Virtual LAN)

۳-۱۳ شناسایی خصوصیات شبکه های اینترا نت و اکسترانت

مقدمه:

یکی از فاکتور های مهم تکنولوژی اینترنت و همچنین اینترانت پروتکل ها هستند که زیر ساخت های مورد نیاز اینترنت را فراهم می آورند. مجموعه پروتکل های مورد نیاز در این ارتباط درمجموعه پروتکل TCP /IP جمع آوری شده است.

این مجموعه از ۲ پروتکل TCP (Transmission Control Protocol) و IP (Internet Protocol) تشکیل شده است. پیش از اتصال به شبکه اینترنت و یا استفاده از شبکه اینترانت پیکربندی کلیه تجهیزات بر اساس پروتکل اجتناب ناپذیر است.تجهیزات مورد نظر اعم است از ایستگاه کاری،مسیریاب و تمامی سیستم هایی که عملیات تادل داده ها را انجام می دهند.

این بخش با معرفی خانواده پروتکل های TCP /IPآغاز می شود، سپس با شناخت خصوصیت های IP و نحوه اختصاص آن و همچنین کلاس بندی IP ادامه پیدا می کند و با چگونگی پیکربندی TCP /IP در Windows 2000 به پایان خواهد رسید.

آشنایی با TCP /IP

از آنجا که این پروتکل مهمترین شرط ورود به دنیای اینترنت است می بایست خصوصیات این پروتکل را به دقت فراگیرید.ابتدا با تاریخچه پروتکل آغاز می نماییم.

تاریخچه TCP /IP

این پروتکل در سال ۱۹۷۳ معرفی گردید ،سپس به مرور زمان تغییرات بسیاری بر روی آن انجام گردید.در سال ۱۹۷۸ به ۲ پروتکل مجزای TCP وIP تقسیم شد و با گذشت زمان روز به روز محبوب تر گردید تا آنجا که در سال ۱۹۸۳ به عنوان پروتکل استاندارد برای ARPAnet معرفی گردید.

عمده کارهای تحقیقاتی مربوط به استاندارد ها و پروتکل ها در دانشگاه کالیفرنیا- برکلی انجام می شد.همزمان با این تحقیقات در دانشگاه برکلی ،تحقیقات بر روی نسخه لینوکس این دانشگاه که به " BSD " معروف بود هم انجام می شد. با اضافه کردن پروتکل به این نسخه از لینوکس ،آن را برای استفاده در محیط های تحقیقاتی و آموزشی آماده کردند.

این پروتکل در بین کارشناسان معمولا به عنوان "خانواده اتصال های بدون اشکال "شناخته می شود.

اهداف طراحی پروتکل TCP /IP:

- طراحی یک پروتکل که مستقل از سازندگان سخت افزار باشد.در حال حاضر این پروتکل از مقدمات و ملزومات شبکه است که تمامی سازندگان تجهیزات شبکه خود را ملزم به رعایت آن می دانند.
- پروتکل می بایست قابلیت رفع اشکالات بوجود آمده در ارتباط را دارا باشد بدین معنی که اگر داده ها بصورت کامل و صحیح به مقصد نرسیدند ،نواقص داده ها را اصلاح نماید.
- این پروتکل ابتدا برای مقاصد نظامی طراحی شده بود و می بایست در صورت خروج بخشی از شبکه از مدار (مانند حمله دشمن به شهر یا مرکز نظامی)دیگر بخش ها بدون مشکل به فعالیت ادامه دهند.
- در صورت برقراری شبکه بین دونقطه ، این ارتباط را بدون مشکل برقرار نگاه دارد.
- بار شبکه را حتی الامکان پایین نگاه دارد. بسته های این پروتکل حجمی معادل ۲۰ بایت دارند که این امر تضمین می کند بار شبکه افت پیدا کند.
- اجازه افزایش کاربران و توسعه شبکه بدون متوقف شدن عملکرد و یا بروز اختلال در عملکرد شبکه را داشته باشد.
- از مجموع اهداف فوق می توان نتیجه گرفت که با استفاده از این پروتکل امکان انتقال داده ها بصورت دقیق و عاری از هرگونه اشکال بین سیستم ها انجام می پذیرد.

شبکه های اینترانت و اکسترانت :

شاید این تیتر کمی نامعمول و یا حتی گیج کننده باشد.ولی در این بخش در خصوص این مفاهیم سخن می گوییم تا این ابهام برطرف شود.

همانگونه که می دانید کلمه "اینترنت "کوتاه شده ی کلمه" اینترنتورک " می باشد که امروزه مشتقات فراوانی از آن ساخته شده و در اصطلاحات شبکه به کار می رود.

ابتدا کمی در مورد مفهوم اینترنتورک با هم سخن می گوییم تا مطمئن شویم که این مفهوم کاملا روشن بیان شده است زیرا درک مفهوم تمامی مشتقات در گرو شناخت این مفهوم است.

شبکه ترکیبی است از تجهیزات مختلف که با یک استاندارد خاص در کنار هم قرار داده شده اند.برای برقراری ارتباط می بایست کلیه اجزا با هم اتصال داشته و قادر به تبادل اطلاعات باشند.این ارتباط داخلی اجزا و تبادل اطلاعات با یکدیگر را در اصطلاح "اینترنتورک "می گویند.

شبکه اینترنت هم از این ساختار استفاده می کند. این شبکه از مسیریاب هایی که در لایه سوم عمل می کنند ، بهره مند است که می تواند با برقراری ارتباط توسط پروتکل TCP/IP ارتباطی در مقیاس بسیار وسیع را برقرار سازد.

مفهوم دیگر این بخش اینترانت است. این لغت به معنی برقراری ارتباط و تبادل داده ها درون یک شبکه می باشد. با این تعریف به راحتی می توان تفاوت بین اینترنت و اینترانت را درک کرد.

مفهوم " اینترا" به معنای داخل ودرون می باشد. حال می توان اینترانت را به راحتی تعریف کرد.اینترانت شبکه ای است محدود که افراد درون آن شبکه از امکان اتصال به شبکه برخوردار هستند و مدیریتی واحد بر آن مدیریت و نظارت دارد.

حال به سراغ مفهوم دیگر یعنی "اکسترانت " می رویم. در این ساختار ما تعدادی شبکه مجزا داریم که هرکدام مدیریت مجزا دارند و همگی می توانند با یکدیگر تبادل داده انجام دهند. در واقع با بیان دیگر می توان گفت که این ساختار نمونه توسعه یافته ی شبکه اینترانت است. این شبکه ها نوعی همکاری و هماهنگی علیرغم وجود یک سیستم مدیریت واحد دارند. مونه این ساختار را می توان در سیستم های خدمات پس از فروش شرکت های خودرو سازی مشاهده نمود که هر شهری سیستمی با مدیریت محلی و در عین حال عضو شبکه اصلی شرکت می باشد.

مزایای استفاده از TCP/IP بر پروتکل های دیگر :

- این پروتکل کاملا مستقل از شرکت های سخت افزاری و نرم افزاری می باشد.
- این پروتکل امکان تبادل داده ها بین سیستم هایی با سیستم عامل مختلف را فراهم می آورد.
- این پروتکل می تواند بدون محدودیت در زیر ساخت شبکه از جمله اترنت ،توکن رینگ و X.25 تبادل داده ها را انجام دهد.
- این پروتکل قابل مسیریابی است یعنی می تواند بهترین مسیر را انتخاب کرده و مانع ایجاد ترافیک در شبکه گردد.
- این پروتکل امکان برقراری ارتباطی مطمئن و قابل اعتماد را فراهم می سازد.
- این پروتکل برای آدرس دهی سیستمی را استفاده می نماید که می تواند شبکه های بسیار بزرگ نظیر اینترنت را هم آدرس دهی نماید.

در این بخش می خواهیم بررسی نماییم که TCP و IP چگونه با یکدیگر کار می کنند

TCP :Transmission Control Protocol

بخش انتقال پروتکل می باشد و همچنین وظیفه برقراری ارتباط مطمئن را نیز بر عهده دارد. بدین منظور داده ها به بخش های کوچکتری تقسیم می نماید که ارسال داده ها را به سهولت انجام داده و ترافیک شبکه را نیز کاهش دهد و پس از رسیدن به مقصد مجدد به هم متصل می نماید. یکی از مقاصد این کار این است که اگر در عملیات انتقال مشکلی پیش آمد نیاز به ارسال کل داده نبوده و تنها همان بخش مجدد ارسال می گردد.

پس از اتمام مرحله تبادل داده ها ؛ بررسی می گردد که آیا داده ها بصورت کامل و بدون اشکال رسیده است ، در صورتی که مشکلی وجود نداشت ارتباط قطع شده و یا اقدام به ارسال داده های دیگر می نماید.

در تصویر زیر نمودار داده ها در پروتکل TCP را مشاهده می نمایید.

ساختار TCP

پورت مقصد		پورت مبدا	
شماره ترتیب			
شماره تاییدیه			
پنجره	پرچم	رزرو شده	افست
اشاره گر فوری		تایید نهایی	
لایه	انتخاب ها		
شروع داده			

پروتکل های لایه اینترنت :

پروتکل های مختلفی در لایه اینترنت عمل می نمایند که ۳ پروتکل عمده آنها را در این بخش با هم بررسی می نماییم.

- Internet Protocol (IP)
- Internet Control Message Protocol (ICMP)
- Address Resoloution Protocol (ARP)

: Internet Protocol (IP)

شاید اگر بگوییم مهمترین پروتکل لایه اینترنت همین پروتکل IP است خیلی بزرگنمایی نکرده ایم.توسط این پروتکل داده ها از نقطه از شبکه به نقطه دیگر منتقل می شوند که این عمل را مسیریابی می گویند.

در واقع پروتکل IP مستقل از اتصال است بدین معنی که نیازی به برقراری ارتباط اولیه بین دونقطه وجود ندارد بررسی و نظارت بر روی چگونگی ارسال و مشکلات احتمالی بر عهده ی TCP می باشد. و IP تنها وظیفه مسیریابی و رساندن داده ها به مقصد از پیش تعیین شده را برعهده دارد.

> IP را می توان کاملا غیر قابل اطمینان دانست زیرا هیچ نظارتی بر روی داده های ارسال ندارد و نمی تواند مشکلات احتمالی را مشاهده و تصحیح نماید. و لی در مقابل TCP به دلیل برخورداری از سیستم نظارتی قوی مشکلات را مشاهده و اشکالات پیش آمده در مرحله انتقال را برطرف می سازد از این رو TCP را می توان کاملا قابل اطمینان دانست.

IP مسیر و مقصد نهایی را به داده ها اضافه می کند ، بدون این آدرس ها مسیر یاب های بین راه و درگاه خروجی نمی توانند داده ها را تا مقصد هدایت نمایند.

ساختار IP

نسخه پروتکل IP	طول ساختار	نوع خدمات	طول ساختار	
بخش شناسایی			علامت	بخش های افست
عمر بسته	پروتکل		تایید نهایی ساختار	
آدرس IP مبدا				
آدرس IP مقصد				
انتخاب ها و لایه ها				
ساختار TCP شروع داده				

:Internet Control Message Protocol

همانند پروتکل های قبلی ،این پروتکل هم در لایه شبکه عمل می نماید و وظیفه آن مدیریت و نظارت در این لایه است.مسیریاب ها بر روی داده هایی که بصورت کامل و صحیح به مقصد نرسیده اند پیامی قرار می دهد و توسط این پروتکل به فرستنده ارسال می کند که فرستنده آن بسته ی داده را مجدد ارسال نماید. نمونه های دیگری از کاربرد های این پروتکل را در فصل ۵ مشاهده خواهید نمود.

: Address Resoloution Protocol

وظیفه این پروتکل تخصیص آدرس IP به آدرس فیزیکی سخت افزار شبکه می باشد. بدین منظور توسط پروتکل IP ، جدولی تهیه می شود که آدرس IP اختصاص یافته به هر آدرس فیزیکی در آن ثبت می شود. هرگاه سیستمی بخواهد که داده ای را برای یکی از سیستم ها ی درون شبکه با کمک آدرس IP آن ارسال نماید ، ابتدا بررسی می شود که این آدرس در جدول موجود است یا خیر، در صورت موجود بودن آن را برای آن سیستم

ارسال می کند که این عمل ترافیک شبکه رابسیار کاهش می دهد. اگر در جدول وجود نداشت در خواستی به شبکه ارسال می گردد تا پس از دریافت پاسخ سیستم از سیستم مورد نظر، داده ها به آن سیستم ارسال گردد.

پروتکل دیگری هم وجود دارد که عملکرد آن درست برخلاف این پروتکل Reverse AddressResoloution)

(Protocol است که به اختصار RARP گفته می شود. هرگاه آدرس IP در لیست موجود نباشد هماتگونه که گفته شد درخواستی برای مشخص شدن آن به شبکه ارسال می شود. این درخواست به همراه داده ها در سرور شبکه ذخیره می شود تا پس از مشخص شدن IP برای آن سیستم ارسال شود.

مسیریاب و مسیریابی :

هماتگونه که آموختید ، مسیریابی در واقع فرآیند انتقال داده از یک نقطه شبکه به نقطه دیگر آن است.این فرآیند بسیار شبیه رانندگی است. شما قبل از حرکت میبایست بررسی نمایید که کدام مسیر شما را در کوتاهترین زمان و بهترین مسیر به مقصد می رساند . البته ممکن است در بین مسیر تصمیم شما تغییر کند که این تغییر مسیر شما را هم تغییر می دهد.در شبکه ، آدرس گیرنده به داده ها افزوده می شود و این بسته حاوی آدرس گیرنده به درگاه خروجی شبکه ارسال می گردد.



نکته بسیار مهمی که باید آن را به خاطر بسپارید این نکته است که درتمامی مطالب مربوط به اینترنت که مطالعه می نمایید هرگاه صحبت از درگاه خروجی به میان آمد لازم است توجه نمایید درگاه خروجی یک مسیریاب است و عمل مسیریابی را هم انجام می دهد.

هر سیستم در شبکه دارای یک درگاه خروجی پیش فرض است که تبادل داده ها از طریق این درگاه صورت می پذیرد.هر مسیریاب دارای جدولی است که شبکه های نزدیک خود را در آن ثبت و ضبط نموده که داده ها را به اولین مسیریاب داده و هرکدام از مسیریاب های شبکه داده ها را دست به دست نموده تا به مقصد نهایی برسد. به مسیر طی شده از مبدا به مقصد " مسیر " یا " Route" می گویند.

پروتکل های لایه کاربردی (Application):

این پروتکل ها در بالاترین لایه مدل یا همان لایه کاربردی قراردارند و برخی از آنها بسیار معروف هستند و بسیار مورد استفاده قرار می گیرد.برخی از این پروتکل ها به شرح ذیل هستند که در این بخش با این پروتکل ها و موارد استفاده آنها بیشتر آشنا می شویم:

- FTP
- SFTP
- POP3
- LPD
- TELNET
- HTTP
- NTP
- SCP
- IGMP
- SNMP
- TFTP
- SMTP
- IMAP
- NFS
- SSH
- HTTPS
- NNTP
- LDAP
- LPR

Simple Network Management Protocol (SNMP) :

این پروتکل از مجموعه پروتکل های مدیریتی شبکه است که به مدیر شبکه اجازه می دهد تا اطلاعات مربوط به شبکه را جمع آوری کند.این پروتکل اطلاعات مربوط به تجهیزات شبکه مانند هاب , مسیریاب ,پل های ارتباطی و بطور کلی همه اجزای موجود و فعال شبکه را جمع آوری می نماید. این پروتکل برای برقراری ارتباط و جمع آوری داده ها از پروتکل UDP استفاده می نماید.

File Transfer Protocol (FTP) :

این پروتکل ساختاری برای انتقال داده ها بین سیستم های رایانه ای را ممکن می سازد. این سیستم از پروتکل TCP استفاده می نماید تا صحت انتقال داده ها را تضمین نماید.

Trivial File Transfer Protocol (TFTP) :

این پروتکل نسخه محدود پروتکل FTP می باشد که ساختار حفظ شده اما بسیاری از امکانات FTP در این نسخه برای کمتر کردن حجم حذف شده است.و برای انتقال داده ها بین مسیریاب ها استفاده می شود. این سیستم از پروتکل UDP استفاده می نمایدتا سرعت انتقال داده ها را افزایش دهد اما انتقال داده ها قابل اطمینان نبوده و صحت انتقال تضمین نمی گردد.

: Secure File Transfer Protocol (SFTP)

این پروتکل زمانی مورد استفاده قرار می گیرد که می خواهیم داده ها را بر روی یک شبکه کد گزاری شده منتقل نماییم.بدین منطور از SSH برای کد گزاری داده ها استفاده می نماید (مراحل را در بخش های بعدی خواهیم دید.)و داده های کد گزاری شده را دقیقا همانند ساختار FTP بین سیستم ها منتقل می نماید.

: Simple Mail Transfer Protocol (SMTP)

این پروتکل وظیفه انتقال پست الکترونیکی بین سرور های پست الکترونیکی را بر عهده دارد. البته برای این منظور سرویس دهنده ها از ۲ پروتکل POP و IMAP4 هم استفاده می نماید.

: Post Office Protocol (POP)

این پروتکل مکانیزمی بسیار قوی را برای پست الکترونیکی ورودی به سیستم کاربر بکار می بندد. آخرین نسخه آن ، نسخه ۳ است. در این مکانیزم ، تمامی نامه های ورودی بر روی سیستم رایانه فرد ذخیره می شود. در این مرحله هیچ انتخابی برای کاربر وجود نخواهد داشت. پس از اتمام ذخیره ,کاربر می تواند پس از بررسی برخی از این نامه ها را حذف نماید.

: Internet Message Access Protocol ,Version 4 (IMAP4)

این پروتکل اجازه انتخاب نامه ها جهت ذخیره بر روی سیستم ها را می دهد که امکانی بسیار کاربردی نسبت به POP می باشد . جستجو بین نامه های دریافتی و سیستم کنترل دسترسی بسیار پیشرفته دیگر امکانات این پروتکل است.از این رو می توان این پروتکل را بسیار پیشرفته تر از POP دانست.نسخه فعلی این پروتکل ,نسخه ۴ است.

: Line Printer Daemon (LPD)

یکی دیگر از پروتکل های مورد استفاده را می توان این پروتکل دانست. این پروتکل بر روی سرور های چاپ و یا چاپگر ها قرار می گیرد و پس از دریافت درخواست چاپ از رایانه کاربر, آن را به چاپگر فرستاده تا عمل چاپ انجام میگیرد.

با توجه به این نکته که TCP/IP بر روی UNIX هم عمل می نماید, این سرویس بر روی این سیستم عامل هم عمل می نماید.

: Network File System (NFS)

در سیستم عامل UNIX نحوه دسترسی به فایل ها منحصر بفرد است. این پروتکل به منظور انجام این عمل طراحی شده است. توسط این پروتکل رایانه های مبتنی برUNIX امکان دسترسی به مطالب و فایل های اشتراکی قرار داشته بر روی شبکه را خواهند داشت.

: TELNET

این پروتکل یک شبیه ساز ورود به شبکه است که امکان ورود به سیستم از راه دور بر روی بستر TCP/IP را فراهم می سازد. این پروتکا امکان ورود به سیستم , اجرا و یا حذف نرم افزار ها بر روی سرور و انتقال داده ها را از سرور با کمک سیستم کد گزاری بسیار قوی فراهم می آورد.

: Secure Shell (SSH)

این پروتکل به منظور برقراری یک ارتباط امن TELNET بر روی بستر TCP/IP مورد استفاده قرار می گیرد.موارد استفاده آن همانند TELNET می باشد با این تفاوت که نوع ارتباط امن است و تبادل داده ها بصورت کد گزاری شده انجام می گردد.

: Hyper Text Transfer Protocol (HTTP)

این پروتکل سیستم نظارت و مدیریت است که برای مدیریت برقراری ارتباط بین مرورگر صفحات وب و سرور وب مورد استفاده قرار می گیرد.زمانی که شما درخواست نمایش یک صفحه وب را به اینترنت می فرستید, این صفحه ترکیبی از نوشته ها , تصاویر و مطالب چند رسانه ای می باشد که این پروتکل مدیریت نمایش این مطالب در یک صفحه واحد را بر عهده دارد.

: Hyper Text Transfer Protocol Secure (HTTPS)

نسخه امن پروتکل می باشد. این پروتکل مکانیزمی برای ارتباط و تراکنش با امنیت بالا برای ارتباط مرورگر و سرور ارایه می نماید. که امکان تبادل داده ها بصورت کدگزاری شده و تصدیق کلمه عبور را فراهم می آورد.

: Network Time Protocol (NTP)

این پروتکل نخستین بار توسط پروفسور دیوید مایلز از دانشگاه دلاویر بنا نهاده شد. این پروتکل برای همسان سازی زمان رایانه با زمان استاندارد و یا زمان تعیین شده از سوی سرور استفاده می گردد. یکی از محاسن این کار یکسان سازی زمان تمام رایانه های موجود در یک شبکه می باشد زیرا ممکن است بسیاری از تراکنش های شبکه وابسته به زمان بوده و می بایست در زمانی معین انجام پذیرد.

: Network News Transfer Protocol (NNTP)

این پروتکل به منظور دسترسی به اخبار در شبکه اینترنت که بصورت طبقه بندی شده در گروه های خبری مختلف از جمله :سیاست ,ورزش ،فناوری اطلاعات ، رایانه و ... وجود دارند، بکار می رود.

: Secure Copy Protocol (SCP)

شاید FTP را بتوان آسانترین شکل انتقال فایل ها دانست اما یکی از معایب این کار عدم وجود یکی سیستم امنیتی مناسب در این روش است. کد کاربری و کلمه عبور بدون کد گزاری منتقل می نماید که راه را برای سوء استفاده را باز می گزارد.

پروتکل SCP به منظور رفع این مشکل بنا نهاده شد.برای کدگزاری و برقراری ارتباط امن از SSH استفاده می شود که این امر تضمین می کند داده ها بصورت کاملا امن منتقل می شوند.

: Lightweight Directory Access Protocol (LDAP)

در شبکه های بزرگ ، مدیر شبکه به منظورنگهداری سوابق کاربران و منابع شبکه نیازمند تهیه یک فهرست جامع است که بدین منظور نیازمند یک استاندارد است که متکی به فرد یا یک نرم افزار خاص نباشد. از این روپروتکل LDAP به عنوان یک استاندارد مطرح شد.

: Internet Group Management Protocol (IGMP)

این پروتکل به منظور شناخت ساختار شبکه و گروه های موجود شبکه استفاده می شود. با استفاده از پیام های ارسال شده توسط این پروتکل دقیقا می توان معین نمود که رایانه دریافت کننده در کدام گروه قرار دارد.

: Line Printer Remote (LPR)

هرگاه برای به اشتراک قراردادن چاپگر در شبکه ازLPR استفاده نماییم،جهت ارتباط رایانه کاربر با چاپگر شبکه از LPD در سمت کاربر استفاده می نماییم که ارتباط با چاپگر را مدیریت نماید.

دیگر پروتکل های لایه های بالایی :

پروتکل های دیگری هم در لایه های بالایی وجود دارند که نقش بسیار مهمی را در پروتکل TCP/IP ایفا می نمایند که برخی از آنها را در این بخش بررسی خواهیم نمود:

- UDP
- SMB
- AFP
- ICS

: User Datagram Protocol (UDP)

این پروتکل در لایه انتقال فعال بوده و از گروه پروتکل های مستقل از اتصال است.به این دلیل امکان برقراری ارتباطی سریع ولی غیر قابل اعتماد را فراهم می سازد.این پروتکل برای پخش تصاویر ویدئویی آنلاین و رادیو های اینترنتی از این پروتکل استفاده می شود.

: Server Message Block (SMB)

این پروتکل به منظور ارسال پیام های کاربران به سرور است.این پیام ها می تواند به منظور دسترسی به یک وب سایت؛ مشاهده منابع به اشتراک قرارداده شده و یا استفاده از چاپگر های شبکه باشد.

: Samba

پروتکل SMB تنها محدود به سیستم عامل ویندوز نیست بلکه امروزه آن را به بصورت یک پروتکل عام تبدیل نموده است.Samba یک نرم افزار کد باز است که در شبکه های مبتنی بر لینوکس و یونیکس کاربرد دارد. کاربرد سامبا برقراری ارتباط بین کاربران شبکه ویندوز با سرور های مبتنی بر لینوکس و یونیکس بر اساس پروتکل TCP/IP می باشد.

AppleTalk Filling Protocol (AFP):

بسیار قبل تر از آنکه ویندوز سیستم اشتراک فایل ها را معرفی کند ؛این سیستم توسط Appleبرای پروتکل AppleTalk مورد استفاده قرار می گرفت.

این پروتکل دسترسی کاربران ویندوز به فایل های اشتراکی در سیستم هایی که از AppleTalk استفاده می نمایند را ایجاد می نماید.

Internet Connection Sharing (ICS):

بعد از نسخه ۹۸ ویندوز ،همه نسخه ها دارای سرویس اشتراک قراردادن اینترنت یا ICS هستند.این سرویس امکان اشتراک اینترنت یک سیستم به دیگر کاربران شبکه را فراهم می نماید.

یکی از مهمترین محاسن این سرویس امکان استفاده از درگاه خروجی نرم افزاری به جای مسیریاب است که می تواند صرفه جویی مالی زیادی برای راه اندازی شبکه های کوچک باشد.

پورت ها در پروتکل TCP/IP :

در پروتکل TCP/IP فرستنده داده ها را از پورت یا درگاه خاصی ارسال نموده و در گیرنده در پورت خاصی دریافت می شود. در واقع پورت یک نشانگر عددی است که نشان می دهد داده های مربوط به هر نرم افزار کاربردی باید چگونه ارسال یا دریافت گردد.

هر پورت یک نشانگر عددی دارد که می تواند عددی بین ۰ تا ۶۵۵۳۵ باشد. پورت ها می توانند TCP یا UDP باشد. هرکدام دارای یک لیست جداگانه از پورت ها هستند که تضمین نماید هیچ خللی ایجاد نشود.یکی از محاسن این کار این است که چندین پروتکل همزمان در یک سیستم فعال باشند بدون اینکه در وظایف یکدیگر خللی ایجاد نمایند.

به منظورسهولت استفاده کاربران ازسرویس ها و پورت ها؛ استاندارد سازی شده است و برای پورت ها شماره ای در نظر گرفته شده است که در همه جا یکسان است.

برخی از پورت های مشهور را در جدول زیر مشاهده می نمایید :

UDP		TCP	
پروتکل	شماره پورت	پروتکل	شماره پورت
NETSTAT	PORT 15	FTP data	PORT 20
TFTP	PORT 69	FTP control	PORT 21
RPC	PORT 111	SSH	PORT 22
NetBIOS name service	PORT 137	Telnet	PORT 23
SNMP	PORT 161	SMTP	PORT 25
DNS queries	PORT 53	DNS zone transfer	PORT 53
RIP	PORT 520	Gopher	PORT 70
NFS	PORT 2049	Finger	PORT 79
NETSTAT	PORT 15	HTTP	PORT 80
		POP 3	PORT 110
		NNTP	PORT 119
		NTP	PORT 123
		IMAP4	PORT 143
		HTTPS	PORT 443

پروتکل هایی که در سمت کاربران فعال هستند هم نیاز به پورت برای تبادل داده ها دارند اما نمی توانند از این پورت ها استفاده نمایند از این رو از پورت های بین ۱۰۲۴ و ۴۹۱۵۱ که آنها را پورت های ثبت شده می نامند استفاده می کنند.

ترکیب آدرس IP و شماره پورت را " سوکت " می نامند. ایجاد یک سوکت در سمت فرستنده ویک سوکت در سمت گیرنده برای برقراری ارتباط در پروتکل TCP ضروری است. سوکت در پروتکل Novel NetWare بخشی از آدرس است که معمولا بصورت پویا برای هر داده ارسال شده اختصاص داده می شود.

اولین بار سوکت در هسته اصلی یونیکس BSD ایجاد شده بود که هدف آن تبادل داده ها بین دو سیستم در دو فضای مختلف بود که ارتباط ایجاد شده در یک زمان دوطرفه باشد یعنی همزمان ارسال و دریافت انجام شود.

آشنایی با سیستم آدرس دهی IP :

همانگونه که می دانید ؛ آدرس دهی IP همانند سیستم آدرس دهی شهری است که با این روش مقصد داده ها در شبکه را صرفنظر از پروتکل TCP یا UDP می توان مشخص نمود.

امروزه ۲ ساختار برای ارایه آدرس های وجود دارد : نسخه ۴ پروتکل IP و نسخه ۶ پروتکل IP که با تفاوت های آنها در این بخش آشنا خواهیم شد.

پیش از ورود به این مبحث تفاوت بین آدرس IP و آدرس Ethrenet که در اکثر اوقات باعث سر درگمی کاربران می شود را بررسی می نماییم :

آدرس Ethrenet :

آدرس Ethrenet همان آدرس فیزیکی تجهیزات ارتباطی شبکه (MAC) می باشد که در مباحث پیش آموختیم. شناسه ای منحصر بفرد است که توسط شرکت سازنده به تجهیزات شبکه اختصاص داده می شود که قابل تغییر هم نیست. با این توضیح و آشنایی با خصوصیات آدرس IP براحتی تفاوت میان این دو ساختار آدرس دهی روشن و واضح خواهد بود.

نسخه ۴ آدرس IP :

آدرس IP عددی است در مبنای ۱۰ که این آدرس به ۴ بخش تقسیم شده که هر بخش با یک نقطه از بخش دیگر جدا می شود. عدد های قرار گرفته در هرکدام از این ۴ بخش بین ۰ تا ۲۵۵ هستند که شمای کلی آن به این شکل است :

XXX.XXX.XXX.XXX

کلاس بندی های IPV4 :

آدرس های موجود در شبکه های عمومی مانند اینترنت همگی منحصر بفر بوده و نشان دهنده شبکه ای است که کاربران در آن قرار دارند. به منظور نظم بخشی به این سیستم ؛کلاس بندی هایی وجود دارد که در این بخش به آنها خواهیم پرداخت.

البته ذکر این نکته ضروری است که برخی از آدرس ها به مقاصد خاصی رزرو شده اند و قوانین مربوط به کلاس ها در مورد این آدرس ها صادق نمی باشد.

کلاس A:

این ساختار مربوط به شبکه های بسیار بزرگ است.امروزه آدرس های این کلاس همگی اشغال شده است.نمونه این شبکه ها جنرال الکتریک ؛ HP ؛IBM ؛Apple ؛ MIT University می باشد. در این کلاس ۱۶,۷۷۷,۲۱۴ آدرس وجود دارد.

آدرس های این کلاس کمتر از 126 .xxx.xxx.xxx هستند.

کلاس B :

این ساختار برای شبکه هایی با مقیاس متوسط در نظر گرفته شده است. در این کلاس ۱۶,۳۸۴ آدرس وجود دارد. نمونه هایی از این شبکه ها میتوان از مایکروسافت نام برد. برخی آدرس ها در این کلاس ممکن است در زمان های خالی شده و به شبکه های دیگری اختصاص یابد.

آدرس 127.0.0.1 برای آزمایش اتصال تجهیزات به شبکه مورد استفاده قرار می گیرد و آدرس های دیگر نیز از لیست آدرس های قابل مسیریابی خارج گردید. استفاده از این آدرس برای آزمایش متاسفانه باعث از بین رفتن ۱۷ میلیون آدرس موجود در این زیر شبکه شده که امروزه ارزش این آدرس ها بیش از پیش احساس می شود.

آدرس های قابل اختصاص در این کلاس از 128.xxx.xxx.xxx آغاز شده و با 191.xxx.xxx.xxx خاتمه می یابد.

کلاس C :

این کلاس آدرس برای شبکه های کوچک مورد استفاده قرار می گیرد. در این کلاس امکان اختصاص 2,097,152 آدرس وجود دارد. آدرس های 192.168.0.0 تا 192.168.255.0 از استثنا های این کلاس هستند که تنها برای شبکه های خصوصی استفاده شده و قابل مسیریابی نیستند.

آدرس ها در این کلاس از 192.xxx.xxx.xxx آغاز شده و با 223.xxx.xxx.xxx خاتمه می یابد.

کلاس D :

این کلاس آدرس های مالتی کست هستند . این آدرس ها تنها به عنوان آدرس مقصد می توانند استفاده شوند و از آنها نمی توان در ساختار داخلی شبکه ها استفاده نمود.

آدرس ها در این کلاس از 224.xxx.xxx.xxx آغاز شده و با 239.xxx.xxx.xxx خاتمه می یابد.

کلاس E :

این کلاس برای مقاصد آموزشی و تحقیقاتی رزرو شده است. آدرس های بالاتر از 239.xxx.xxx.xxx در این کلاس قرار دارند.

نسخه ۶ آدرس IP:

زمانی که آدرس بصورت قراردادی معرفی شد؛ شاید هیچکس روزی را نمی دید که آدرس ها به پایان برسد.پس از رشد سریع کاربران ؛مدیران و سیاست گزاران اینترنت به دنبال راه حلی برای این مشکل بودند که در نهایت نسخه ۶ آدرس IP را معرفی کردند

در این نسخه آدرس ها ۱۲۸ بیتی بوده واعدادی در مبنای ۱۶ هستند که از ۷ بخش که هرکدام با " : " از هم جدا می شوند و در هر بخش ۴ عدد قرار می گیرد؛ تشکیل شده است.

شمای کلی این سیستم به این شرح است :

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

می توان در مجموع ۷۹ اکتیلیون (79,000,000,000,000,000,000,000,000,000) آدرس ایجاد نمود که می تواند نیاز سالهای آینده شبکه ها را مرتفع سازد.

> با توجه به وجود آدرس در نسخه ۴؛نسخه ۶ مراحل آزمایش و تحقیق را طی می نماید و هنوز به صورت رسمی در شبکه ها مورد استفاده قرار نمی گیرداما پشتیبانی از این نسخه بر روی سخت افزار ها تعریف شده است.

آشنایی با مفاهیم زیر شبکه یا Subnetting :

جهت سهولت در مدیریت شبکه ها ؛ مفهوم جدیدی تعریف شده است. هر شبکه را می توان به تعدادی زیر شبکه تقسیم نمود که کاربران آن شبکه ها در داخل شبکه خصوصیات یک شبکه مستقل را داشته باشند. برای روشن شدن این مفهوم با این مثال مبحث را ادامه می دهیم :

یک دبیرستان ممکن است دارای تعداد زیادی دانش آموز باشد که این دانش آموزان با توجه به پایه تحصیلی در کلاس های مختلفی دسته بندی شده اند که هر کلاس یک معلم داشته و درسی خاص می آموزند اما همگی تابع قوانین کلی آن مرکز آموزشی هستند.

استفاده از زیر شبکه ها مزایای زیادی دارد که به برخی از آنها اشاره می نماییم :

- ترافیک درون شبکه را کاهش می دهد.
- کارایی شبکه را بهبود می بخشد.

❖ بهره وری در استفاده از آدرس های شبکه را افزایش می دهد.
❖ امنیت شبکه را تقویت می نماید.

در تقسیم شبکه ها ؛ آدرس ابتدایی و انتهایی هر تقسیم قابل تخصیص نبوده و آدرس های در دسترس همیشه ۲ آدرس کمتر است. به عنوان مثال اگر بخواهیم آدرس های کلاس را به ۴ قسمت تقسیم نماییم به شکل زیر خواهد بود

آدرس شبکه	آدرس ابتدایی	آدرس انتهایی
192.168.0.0	192.168.0.1	192.168.0.63
192.168.0.64	192.168.0.65	192.168.0.127
192.168.0.128	192.168.0.129	192.168.0.191
192.168.0.192	192.168.0.193	192.168.0.255

در این تقسیم ۶۲ آدرس برای هر زیرشبکه و در مجموع ۸ آدرس غیر قابل اختصاص در شبکه وجود دارد. حال اگر این تقسیم را برای ۸ زیر شبکه انجام دهیم آدرس های قابل اختصاص ۳۰ آدرس خواهد بود.

روش دیگری برای نمایش زیر شبکه وجود دارد که به آن CIDR (Classless Inter-Domain Routing) می گویند. در این روش پس از آدرس IP یک " / " قرار می گیرد و پس از آن یک عدد که نمایشگر تعداد بیت های استفاده شده برای آدرس دهی است. در جدول زیر نحوه نمایش در کلاس را مشاهده می نمایید :

تعداد آدرس های موجود	آدرس زیر شبکه	آدرس CIDR
۲۵۴	255.255.255.0	/24
۱۲۶	255.255.255.128	/25
۶۲	255.255.255.192	/26
۳۰	255.255.255.224	/27
۱۴	255.255.255.240	/28
۶	255.255.255.248	/29
۲	255.255.255.252	/30

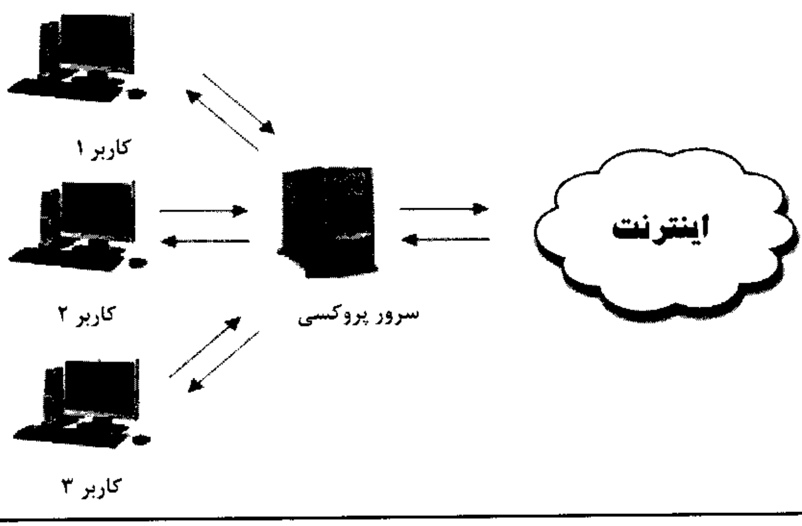
بسیاری از کارشناسان این اعداد را به خاطر می سپارند تا در هنگام کار نیاز به محاسبه این اعداد نداشته باشند.

سرور پروکسی :

استفاده از پروکسی یکی از راه هایی است که شما می توانید برای اتصال شبکه داخلی یا اینترانت خود به شبکه عمومی مانند اینترنت استفاده نمایید. این سرویس به عنوان نماینده شبکه داخلی ترافیک شبکه داخلی را به اینترنت انتقال می دهد. این بدین معنی است که کاربران شبکه داخلی دسترسی مستقیم به اینترنت نداشته و تنها از طریق این سرویس به اینترنت متصل می شوند.

مکانیزم دیگری که می تواند تبادل ترافیک بین شبکه داخلی و اینترنت را انجام دهد دیواره آتش یا فایروال است که از این لحاظ عملکردشان بسیار شبیه هم هستند.

البته عملکرد پروکسی فراتر از یک تبادل داده های ساده است ؛ کارکرد اصلی پروکسی مشاهده و بررسی دقیق داده ها و صدور مجوز برای داده ها و یا جلوگیری از خروج برخی داده ها بر اساس سیاست های امنیتی تعریف شده در شبکه است.



وجود پروکسی زمانی می تواند مفید باشد که تنها مسیر ارتباطی شبکه داخلی و اینترنت از طریق پروکسی باشد. اتصال مستقیم کاربر شبکه داخلی به اینترنت امنیت شبکه را سخت به مخاطره خواهد انداخت.

آدرس های اینترنتی :

به خاطر سپردن یک نام همیشه آسانتر از به خاطر سپردن اعداد مربوط به آدرس IP یک سایت اینترنتی است. از این رو تمامی سایت ها علاوه بر آدرس دارای یک نام هستند که همگان سایت را با آن نام می شناسند.

آدرس های اینترنتی از ۲ بخش تشکیل شده اند : نام سایت و پسوند سایت که نشان دهنده نوع فعالیت آن است. برخی پسوند های مشهور را مشاهده می نمایید :

- .com : پسوند سایت های تجاری
- .edu : پسوند سایت های آموزشی مانند مدارس و دانشگاه ها
- .ir : پسوند سایت های کشور ایران
- .net : پسوند سایت های شبکه های اطلاع رسانی با فعالیت های شبکه ای
- .org : پسوند سایت های سازمانی

ترکیب هر نام و پسوند شبکه کاملا منحصر بفرد است . یعنی ترکیب Tehran.ir فقط یک بار می تواند ایجاد شده و مورد استفاده قرار گیرد. اما هرنام می تواند با پسوند های مختلف هم ایجاد شود. مانند Tehran.org و Tehran.com که ممکن است محتوای نداشته باشد.

تبدیل نام دامنه به آدرس IP :

راه های مختلفی برای انجام این تبدیل وجود دارد که ابتدایی ترین روش آن استفاده از فایلHOST است. در این روش فایل HOST درسیستم عامل ایجاد می شود و در داخل آن اطلاعات مربوط به نام سایت و آدرس IP مربوط به آن ثبت می شود.این فایل می بایست در رایانه تمامی کاربران شبکه ایجاد شود تا سایت مورد نظر در آنها قابل رویت باشد.نمونه ای از اضافه کردن آدرس را مشاهده می نمایید:

217.34.56.45 fserver.com # file server 1

217.34.56.22 mailserver.com # mail server 1

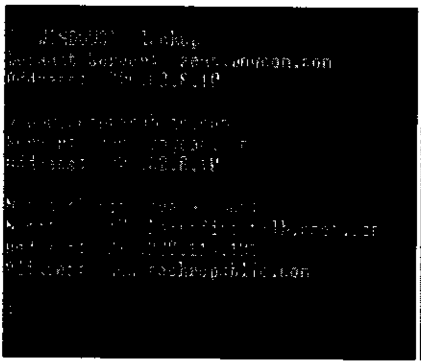
این روش بسیار ساده است اما انجام این کار در تمامی سیستم ها بسیار مشکل و وقت گیر است : از این رو کمتر مورد استفاده قرار می گیرد و به جای آن از روش های جایگزین مانند DNS وWINS استفاده می گردد.

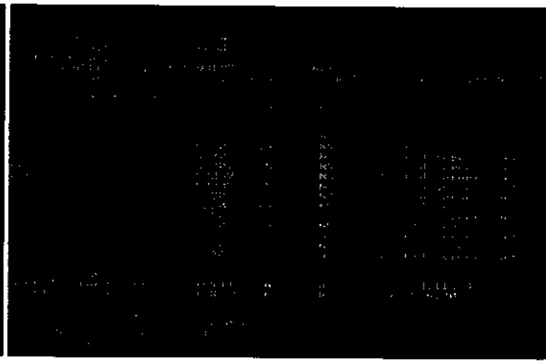
Domain Name Service : DNS

وظیفه اصلی این سرویس ترجمه وتبدیل نام سایت به آدرس و برعکس است.برخلاف مطلب قبلی ؛ این سرویس تنها بر روی سرور تنظیم می شود .و کاربران از این امکان استفاده می نمایند.

مراحل انجام این کار پیچیده و طولانی است وتنها به عملکرد آن اکتفا می نماییم.

دستورات nslookup و dig برای نمایش نحوه سرویس دهی و نمایش مشخصات سرویس دهنده فعال در شبکه است که در فصل بعد کاملا مورد بحث قرار خواهد گرفت.





: Wins

از آنجا که هنوز پروتکل NetBIOS در سیستم عامل ویندوز مورد استفاده قرار می گیرد نیاز به یک سرویس برای تبدیل نام سیستم در پروتکل NetBIOS به آدرس IP احساس می شد. سرویس Wins اسامی سیستم را به آدرس نظیر آن تبدیل می نماید.امروزه به ندرت از این سرویس استفاده می شود.

استفاده همزمان از سرویس های DNS یا WINS و یا استفاده از یکی از این سرویس ها در شبکه بستگی مستقیم به ساختار و نیاز های شبکه دارد و الزامی برای استفاده از هردو سرویس بصورت همزمان وجود ندارد.

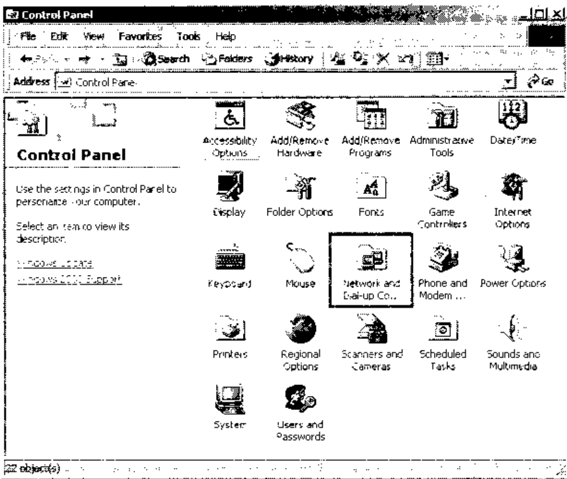
نصب و پیکر بندی TCP/IP در سیستم عامل ویندوز :

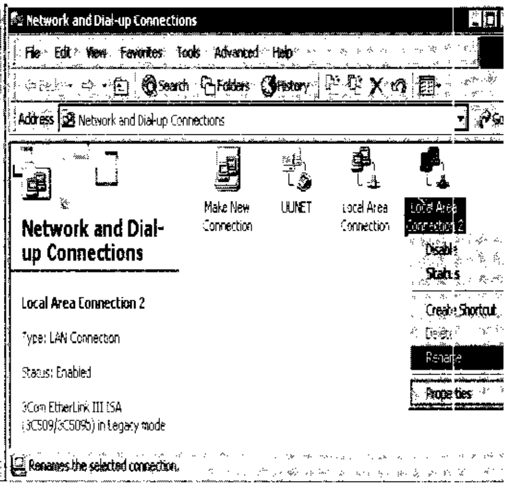
آشنایی با مراحل نصب و پیکر بندی TCP/IP در سیستم عامل ویندوز یکی از ضروری ترین نیاز های یک مدیر شبکه است. در اکثر نسخه های ویندوز این پروتکل به همراه ویندوز نصب می شود اما در این بخش با مراحل نصب و تنظیمات آن آشنا می شویم :

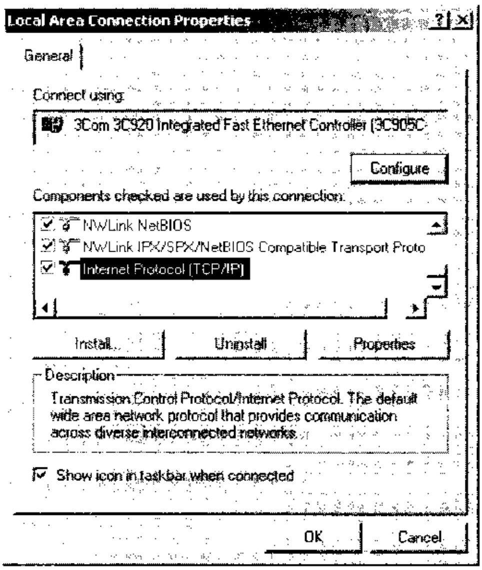
پیش از آغاز مطلب ذکر این نکته ضروری است که در این بخش مبنای ما نسخه ۲۰۰۰ ویندوز است که ازنظر ظاهر با ویندوزXP بسیار متفاوت است اما کلیات این آموزش در هر دو نسخه بسیار شبیه هم است.

برای پیکر بندی TCP/IP مراحل زیر را انجام می دهیم :

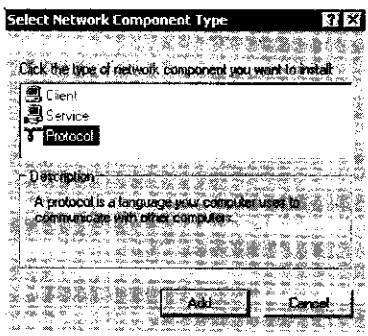
۱= ابتدا وارد مرکز کنترل سیستم می شویم و بخش شبکه را همانند شکل زیر انتخاب می نماییم تا تمامی اتصالات شبکه را مشاهده نمایید. سپس اتصال مورد نظر را انتخاب می نماییم .



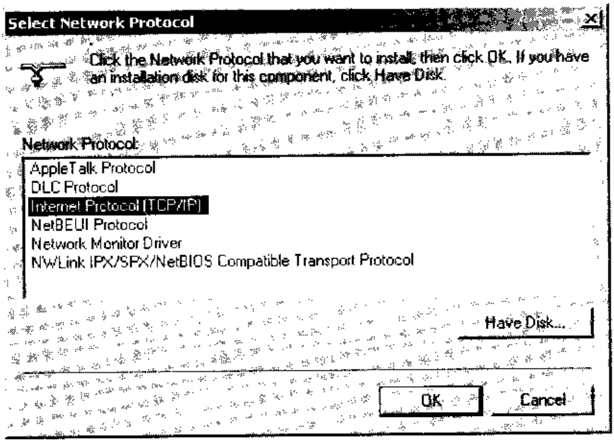




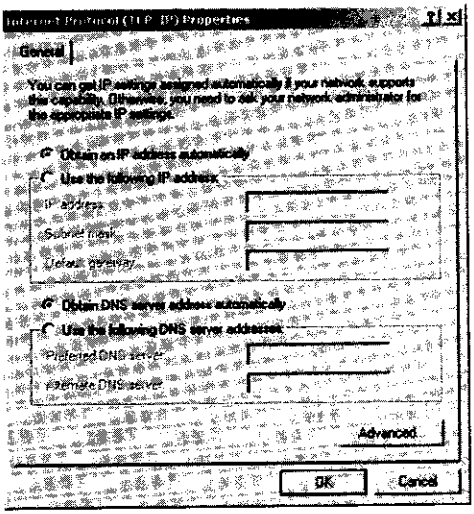
۲- اگر شما TCP/IP را در لیست مولفه های شبکه مشاهده نمی نمایید لازم است مراحل زیر را دنبال نموده تا پروتکل نصب شود اما اگر TCP/IP در لیست موجود است می توانید به مرحله ۴ بروید. برای نصب کلید Install را انتخاب نمایید.



۳- گزینه پروتکل را انتخاب نموده و Add یعنی افزودن را انتخاب می نماییم و پروتکل را جهت نصب انتخاب می نماییم تا پروتکل مورد نظر که همان TCP/IP می باشد ؛ نصب شود.

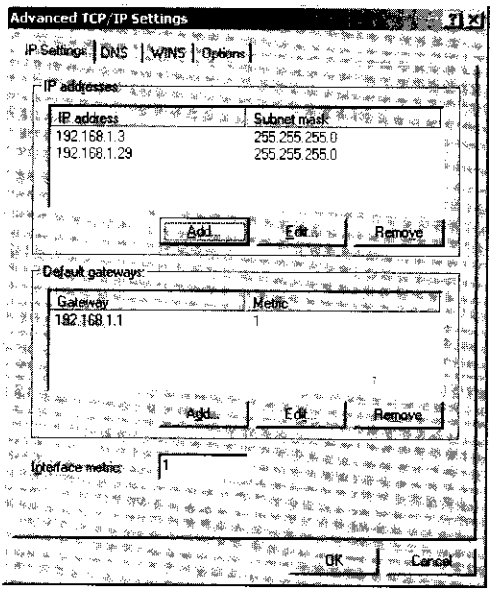


۴- پس از نصب پروتکل ؛ با انتخاب تنظیمات از صفحه اصلی تنظیمات شبکه ؛ شما می توانید آدرس IP مورد نظرخود را در این بخش تعریف نمایید.



۵- در بخش تنظیمات پیشرفته ؛ شما می توانید تنظیمات پیشرفته آدرس IP ؛ مانند تنظیمات سرویس های DNS و WINS را در این بخش انجام دهید.که تنظیمات مربوطه را در این بخش مشاهده خواهید نمود.

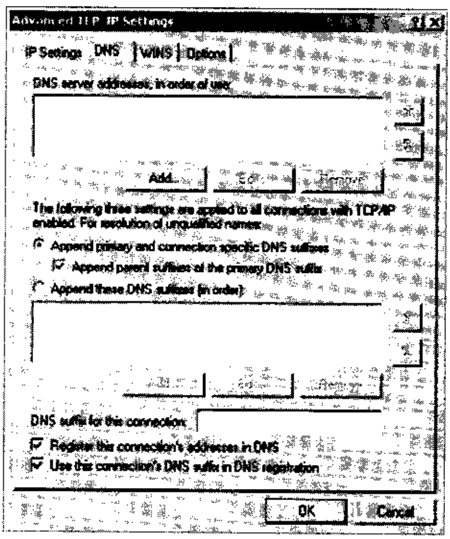
تنظیمات IP :



در این بخش ؛ شما می توانید آدرس های IP را اضافه نموده یا برخی از آنها در صورتیکه آدرس دهی شبکه بصورت خودکار توسط سرویس DHCP انجام می شود را اصلاح نمایید . این کار زمانی مورد استفاده قرار می گیرد که یک سیستم به چندین شبکه متصل بوده و یا چندین سرویس برای کاربران دیگر شبکه بر روی سیستم فعال است.

همچنین شما می توانید درگاه خروجی شبکه و جدول مسیریابی شبکه را نیز در این بخش تنظیم نمایید.

تنظیمات DNS :



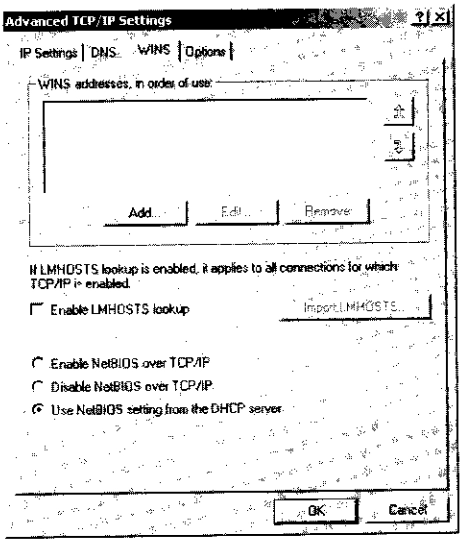
در این بخش تنظیمات مربوط به سرویس دهنده های شبکه را می توان تعریف نمود و با آدرس های جدیدی به این لیست اضافه کرد تا کاربران بتواند از سرویس اینترنت استفاده نمایند .

این تنظیمات می تواند بصورت ایستا و یا پویا بر روی شبکه انجام شود.

تنظیمات WINS :

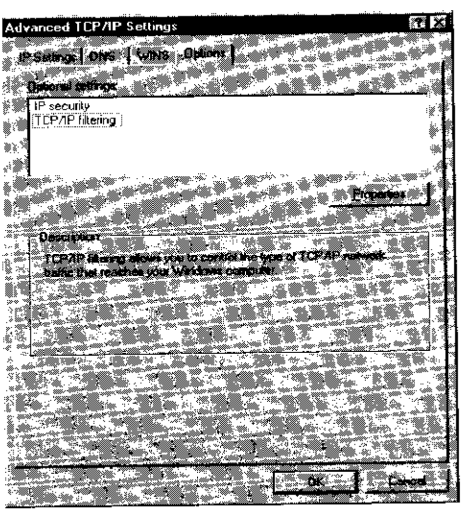
در این بخش آدرس مربوط به سرویس دهنده سرویس WINS را وارد می نماییم.

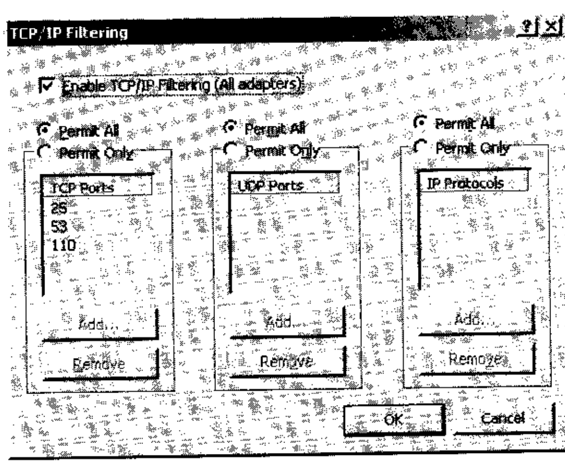
همچنین می توانید استفاده از فایل HOST در سیستم کاربر را فعال یا غیر فعال نمود که در این مورد قبلا صحبت نموده بودیم.



انتخاب ها :

در منوی انتخاب ، شما می توانید تنظیمات امنیتی مربوط به پروتکل IP و یا اعمال تنظیمات و محدودیت بر روی پروتکل TCP/IPرا انتخاب نمایید. با انتخاب تنظیم امنیتی پروتکل IP شما می توانید عملکرد پروتکل امنیتی IPSec را فعال یا غیر فعال نمایید. و همچنین می توانید بر روی پروتکل ها و پورت های خاص محدودیت اعمال نمایید.





ذخیره تنظیمات :

کلیه تنظیمات شبکه در بانک اطلاعاتی رجیستری ویندوز ذخیره می شود و اکثر تنظیمات شبکه را می توان از بخش شبکه در بخش کنترل ویندوز تغییر داد. دراین بخش با برخی تنظیمات و نرم افزار هایی که می توانند تنظیمات شبکه را انجام دهندآشنا می شویم.

تنظیم خودکار (Zero Configuration (ZeroConf :

آیا تاکنون برای شما پیش آمده است تا بخواهید رایانه همراه خود را به شبکه ای متصل نموده تا به عنوان مثال در یک بازی رایانه ای دسته جمعی شرکت نمایید ؟تنظیم چندین پارامتر مانند آدرس IP و تنظیمات سرویس های DNS و WINS همچنین تغییر نام سیستم و عضویت در یک گروه کاری پروسه ای سخت و یا در برخی مواقع غیر ممکن برای کاربران معمولی شبکه است.

با کمک این سرویس شما می توانید تنظیمات مورد نظر را در این پروتکل وارد نموده و آن را بر اساس نیاز پیکر بندی می نمایید و این تنظیمات بدون نیاز به آشنایی کاربر با این روند ؛ بر روی رایانه او نصب نمایید.

تنظیم خودکار اختصاص آدرس IP توسط رایانه :

شما برای تبادل داده ها در یک شبکه نیاز به یک آدرس IP دارید که می تواند بصورت ایستا توسط کاربر انجام شود . یا بصورت پویا توسط سرویس DHCP به رایانه اختصاص داده شود. حال اگر رایانه متصل به شبکه IP خود را به هیچ کدام از راه های ذکر شده دریافت ننمود؛ رایانه آدرسی بین 169.254.1.0 تا 169.254.254.255 را بصورت تصادفی اختصاص می دهد البته در این انتخاب پارامتر هایی مانند آدرس فیزیکی (MAC) هم دخیل هستند که احتمال تداخل آدرس ها را کم نمایند .

البته این آدرس ها ممکن است با بخش های دیگر شبکه که آدرس ایستا یا پویا دارند نتواند ارتباط برقرار نماید تنها با رایانه هایی که از طریق این مکانیزم آدرس خود را دریافت کرده ان ارتباط داشته باشند . این امکان بعد از نسخه ۹۸ ویندوز در همه نسخه ها قرار دارد که آن را سیستم خودکار اختصاص آدرس مجازی با APIPA می گویند.

شبکه داخلی مجازی VLAN:

پس از جایگزینی سوییچ های شبکه به جای هاب ؛ امکان مدیریت بر روی شبکه و ترافیک آن بهینه سازی شد. یکی از این امکانات شبکه داخلی مجازی است که به کاربران این اجازه را می دهد تا کاربرانی که به یک پورت

شبکه متصل هستند امکان ایجاد یک شبکه داخلی بین خود را می دهد.که در بیان دیگر می توان آن را شبکه ای درون شبکه ای دیگر نامید.

این شبکه خصوصیات مربوط به خود راداشته و توسط دیگر کاربران شبکه که در این شبکه قرار ندارند قابل رویت نخواهند بود. به عنوان مثال یک شرکت تمامی بخش های خود را به یک سوییچ متصل می نماید اما هرکدام از بخش های اداری ؛ مالی ؛بازرگانی و پشتیبانی در شبکه های مجازی جداگانه ای قرار خواهند داشت که کاملا مجزا از هم خواهند بود.

جمع بندی:

در این بخش شما:

- ❖ **با مبانی پروتکل TCP/IP آشنا شدید.**
- ❖ **در مورد عملکرد پورت ها و سوکت ها مطالبی آموختید.**
- ❖ **با کلاس بندی های آدرس دهی در شبکه آشنا شدید.**
- ❖ **مفهوم زیر شبکه و نحوه تقسیم بندی زیر شبکه ها را فرا گرفتید.**
- ❖ **در خصوص شبکه مجازی یا VLAN مطالب مفیدی آموختیتد .**

سوالات ارزیابی برای آزمون +Network :

۱ --کدامیک از آدرس ها نمایانگر بخش اول آدرس های سری B می باشد.

الف) ۱ - ۱۲۷
ب) ۱۲۸-۱۹۱
ج) ۱۹۲ - ۲۲۳
د) ۲۲۴- ۲۵۵

۲-کدامیک از این پروتکل ها برای مشاهده صفحات وب لازم است.(تمامی موارد صحیح را مشخص نمایید)

الف) HTTP
ب) HTTPS
ج) FTP
د) DNS

۳-کدام شماره مربوط به پورت POP3 می باشد. .

الف) ۲۵
ب) ۸۰
ج) ۱۱۰
د) ۱۰۰

۴- کدام گزینه در مورد پروتکل TCP/IP صحیح است. (تمامی موارد صحیح را مشخص نمایید)

الف) قابل مسیریابی است
ب) نیاز به برقراری ارتباط دارد.
ج) در شبکه های کوچک مورد استفاده قرار می گیرد.
د) پیکربندی آن بسیار مشکل است.

۵-کدامیک از این پروتکل ها برای ارسال و دریافت پست الکترونیکی کاربرد دارد. (تمامی موارد صحیح را مشخص نمایید)

الف) SMTP
ب) POP3
ج) IMAP
د) TFTP

۶- کدامیک از این موارد هدف اصلی استفاده ازپروکسی است. .(تمامی موارد صحیح را مشخص نمایید)

الف) افزایش امنیت شبکه

ب) افزایش ترافیک شبکه

ج) مدیریت کاربران شبکه

د) محدودیت استفاده کاربران از اینترنت

۷- کدام پروتکل ها برای ارتباط راه دور بکار می رود . (تمامی موارد صحیح را مشخص نمایید)

الف) Telnet.

ب) SCP

ج) SMTP

د) SSH

۸-ارتباط در کدام پروتکل ها امن می باشد . (تمامی موارد صحیح را مشخص نمایید)

الف) SCP

ب) HTTPS

ج) SMTP

د) Telnet

۹- کدام پسوند آدرس اینترنتی نشانگر کشور ایران است . (تمامی موارد صحیح را مشخص نمایید)

الف) net.

ب) org.

ج) ir.

د) com.

۱۰-مزایای استفاده از زیر شبکه می تواند کدام موارد باشد. (تمامی موارد صحیح را مشخص نمایید)

الف) تقسیم بندی ترافیک شبکه

ب) ارتقا امنیت شبکه

ج) افزایش کارآیی شبکه

د) افزایش ترافیک شبکه

پاسخ به سوالات این بخش

۱ - **ب**

همانگونه که در مطالب این بخش ذکر شده آدرس مربوط به کلاس B گزینه ب می باشد.

۲ - **ج**

پروتکل FTP برای نمایش صفحات وب نیست و برای انتقال فایل ها استفاده می شود.

۳ - **ج**

با توجه به توضیحات این فصل مشخص است که پورت POP3 پورت ۱۱۰ است.

۴ - **الف ، ب**

پیکربندی این پروتکل بسیار ساده است و از آن در شبکه های بسیار بزرگ استفاده می شود.

۵ - **الف ، ب ،ج**

پروتکل TFTP برای انتقال فایل ها بکار می رود نه پست الکترونیکی.

۶ - **الف ، د**

استفاده از پروکسی ترافیک شبکه را کاهش می دهد.و کاری برای مدیریت کاربران شبکه انجام نمی دهد.

۷ - **الف،د**

SCP برای کپی بصورت امن استفاده می شود و SMTP هم برای انتقال پست الکترونیک مورد استفاده قرار می گیرد.

۸ - **الف ، ب**

SCP برای کپی بصورت امن استفاده می شود و HTTPS برای اتصال به صفحات وب بصورت امن استفاده می شود.

۹ - **ج**

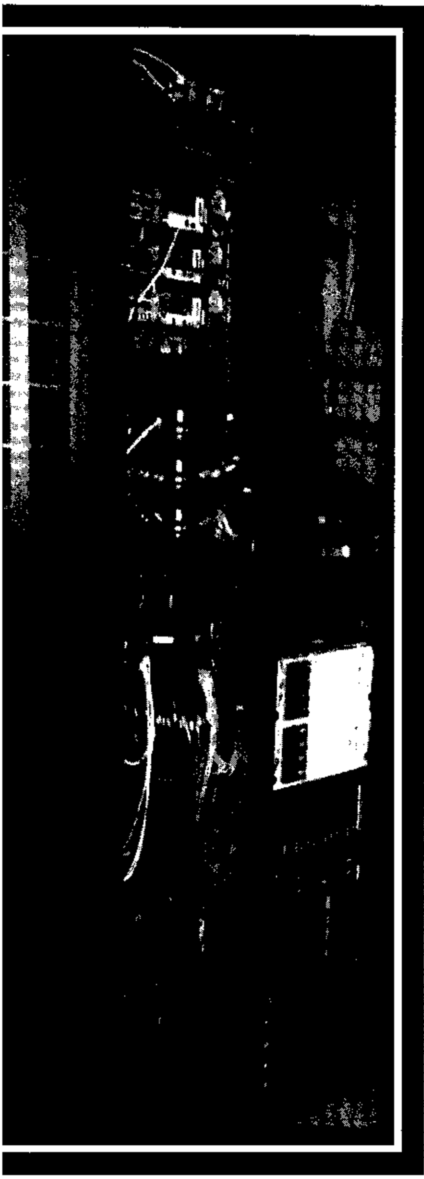
Ir مخفف نام کشور ایران (iran) است

۱۰- **الف ، ب ،ج**

استفاده از زیر شبکه ترافیک شبکه را کاهش می دهد.

فصل چهارم

ابزار کاربردی TCP/IP



شما در این فصل با این مفاهیم آشنا خواهید شد:

۴-۱ شناسایی عملکرد ابزار زیر و انتخاب هرکدام از آنها برای شناسایی و رفع مشکلات شبکه :

- **Tracert/traceroute**
- **ping**
- **arp**
- **netstat**
- **nbtstat**
- **ipconfig/ifconfig**
- **winipcfg**
- **nslookup /dig**

۴-۲ اجرای دستورات بخش ۴-۱

مشاهده خروجی فرامین و تحلیل خروجی آنها جهت شناسایی مشکل و رفع آن

مقدمه:

امروزه کاربران بسیار زیادی از پروتکل در شبکه استفاده می نمایند از این رو آشنایی با ابزار های این پروتکل برای شناسایی مشکلات بوجود آمده و رفع آنها از اساسی ترین وظایف یک مدیر شبکه موفق خواهد بود.

در این بخش سعی خواهیم نمود تا با این ابزار ها بیشتر آشنا شویم

استفاده از ابزار ARP:

ARP یکی از ابزار های پروتکل TCP/IP است .کاربرد این ابزار این است که آدرس IP هر سیستم رابه آدرس فیزیکی آن همانند می سازد. روند انجام این کار به این صورت است که یک بسته فراگیر روی کل شبکه محلی منتشر می کند که در این بسته در حقیقت سوال می شود : سیستمی که آدرس IP مورد نظر را دارد کدام سیستم است و در جواب آدرس فیزیکی آن سیستم را باز می گرداند. آدرس IP و آدرس فیزیکی آن در جدول ARPذخیره می شود که در دفعات بعدی تنها به همان جدول مراجعه خواهد شد.

جدول آدرس های ARP در ویندوز:

دراین جدول آدرس های فیزیکی و آدرس های IP اختصاص داده شده به آنها جمع آوری شده است و در هر مرحله از تبادل داده ها در شبکه داخلی نیازی به انجام جستجویی که در بخش قبلی ذکر شد نخواهد بود.

علاوه بر این مولفه ، زمان قرار داشتن این آدرس ها در جدول هم ثبت می شود به این معنی که سیستم می داند عمر این آدرس چقدر بوده و چه زمانی نیاز به بروز رسانی آدرس ها وجود خواهد داشت.

آدرس ها به دو صورت در این جدول ثبت می شوند :

- ایستا
- پویا

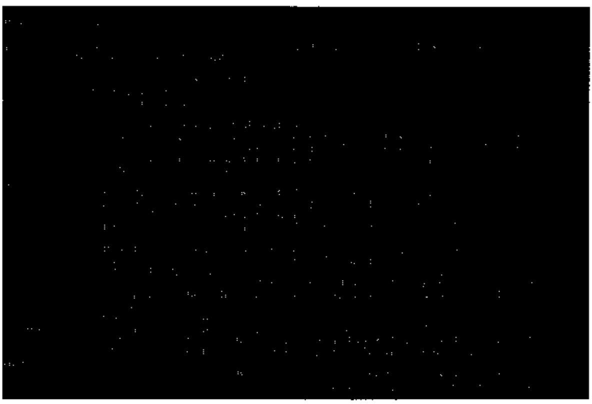
در حالت پویا پس از جستجوی شبکه ؛ موارد یافت شده بصورت خودکار به لیست افزوده می شوند. و پس از سپری شدن عمرشان هم از لیست حذف خواهند شد.کاربر در این مراحل دخالتی نخواهد داشت.

اما در حالت ایستا کاربر آدرس ها را به لیست اضافه و یا حذف می نماید. این مراحل توسط فرمان arp انجام می شود که در این بخش با آن آشنا می شویم.

استفاده از ابزار ARP:

همانگونه که ذکر شد برای افزودن آدرس ها بصورت ایستا در جدول ARP ، از این فرمان استفاده می نماییم.

برخی کلید ها ی ترکیبی نیز وجود دارد که آنها را در شکل روبرو مشاهده می نمایید.



Arp –a:

با اجرای این فرمان ؛ جدول Arp را مشاهده می نمایید همچنین نحوه ثبت آدرس ها را هم می توانید مشاهده نمایید .



اگر سیستم بیشتر از یک کارت شبکه داشته باشد ؛ جدول Arp مربوط به هر کارت شبکه بصورت مجزا نمایش داده می شود.

Arp –s:

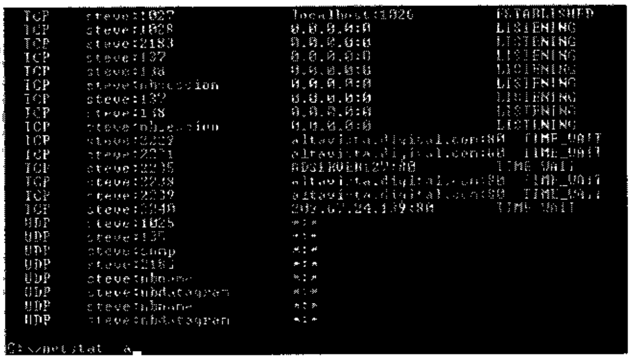
با استفاده از این فرمان می توان آدرس ها را بصورت ایستا به جدول Arp اضافه نمود. شکل این فرمان به شکل زیر می باشد.

```
< arp –s  157.55.85.212  00-aa-00-62-c6-09
```

: Arp –d

برای حذف آدرس از جدول Arp از کلید ترکیبی Arp –d استفاده می شود.

استفاده از netstat :



از این دستور برای نمایش کلیه ارتباطات TCP/IP و نمایش پورتها و آدرس IP فعال درسیستم بکار میرود.

اگر فرمان را بدون کلید ترکیبی بکار ببریم ، خروجی دستور اتصالات شبکه وب را نمایش خواهد داد.

خروجی های های مختلف netstat :

با استفاده از کلید های ترکیبی این فرمان ؛ می توان خروجی های مختلفی را به نمایش قرار داد. لازم به ذکر است که برای اضافه نمودن کلید های ترکیبی؛ بین دستور و کلید باید یک فاصله قرار بگیرد.

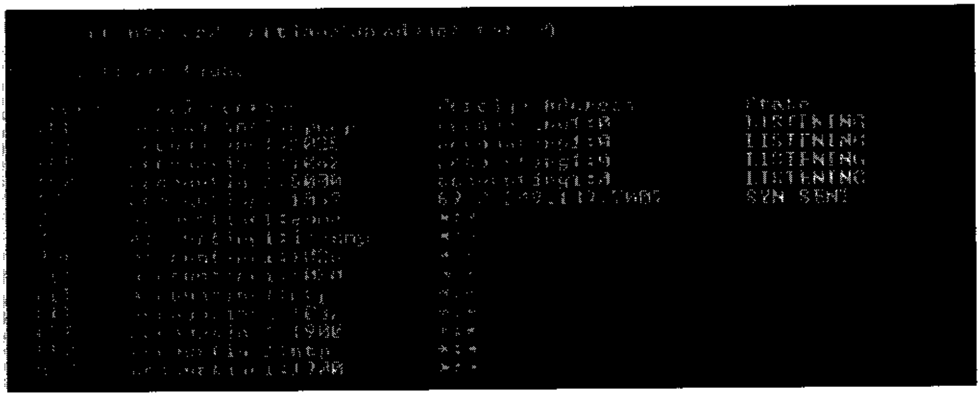
برخی از این کلید های ترکیبی بدین شرح می باشد:

- -a
- -e
- -r
- -s
- -n
- -p

: Netstat --a

در این حالت کلیه اتصالات TCP/IPو UDP نمایش داده می شود.در این نمونه ؛ ستون آخر مربوط به وضعیت اتصال است که در پروتکل UDP همیشه خالی است زیرا این پروتکل نیاز به برقراری اتصال ندارد.

قرار گرفتن * : * در مقابل پروتکل UDP به معنی هر آدرس و هر پورت می باشد.



: Netstat –e

در این حالت ؛ جمع بندی کلی در خصوص ارتباط کارت شبکه به نمایش قرارداده می شود.مولفه هایی مانند حجم داده های ا نتقالی ؛ مشکلات انتقال ؛حجم داده های منتقل نشده نمایش داده می شود.یکی از معایب این نوع نمایش عدم وجود رنگ های مختلف برای نمایش مشکلات است.

```
C:\Users\user>netstat -e
Interface Statistics

                           Received            Sent

Bytes                      93855374        27783081
Unicast packets              145346          162114
Non-unicast packets             286           13194
Discards                          0               0
Errors                            0              15
Unknown protocols                 0
```

: Netstat –r

با این دستور شما می توانید جدول مسیر یابی سیستم را مشاهده نمایید. این دستور بیشتر زمانی کاربرد دارد که رایانه بیشتر از یک کارت شبکه داشته باشد از این رو نمایش نحوه مسیریابی هرکدام اهمیت خاصی دارد.

: Netstat –s

در این حالت شما اطلاعات مربوط به پروتکل های TCP ، UDP ، IP و ICMP را مشاهده می نمایید.

```
C:\Users\user>netstat -s

IPv4 Statistics

  Packets Received                        = 93748
  Received Header Errors                  = 0
  Received Address Errors                 = 0
  Datagrams Forwarded                     = 0
  Unknown Protocols Received              = 812
  Received Packets Discarded              = 419
  Received Packets Delivered              = 196265
  Output Requests                         = 192477
  Routing Discards                        = 0
  Discarded Output Packets                = 6
  Output Packet No Route                  = 628
  Reassembly Required                     = 0
  Reassembly Successful                   = 0
  Reassembly Failures                     = 0
  Datagrams Successfully Fragmented       = 0
  Datagrams Failing Fragmentation         = 0
  Fragments Created                       = 0

ICMPv4 Statistics

                            Received    Sent
  Messages                  289         167
  Errors                    0           0
  Destination Unreachable   282         151
  Time Exceeded             3           0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echo Replies              4           0
  Echos                     0           16
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0
  Router Solicitations      0           0
  Router Advertisements     0           0

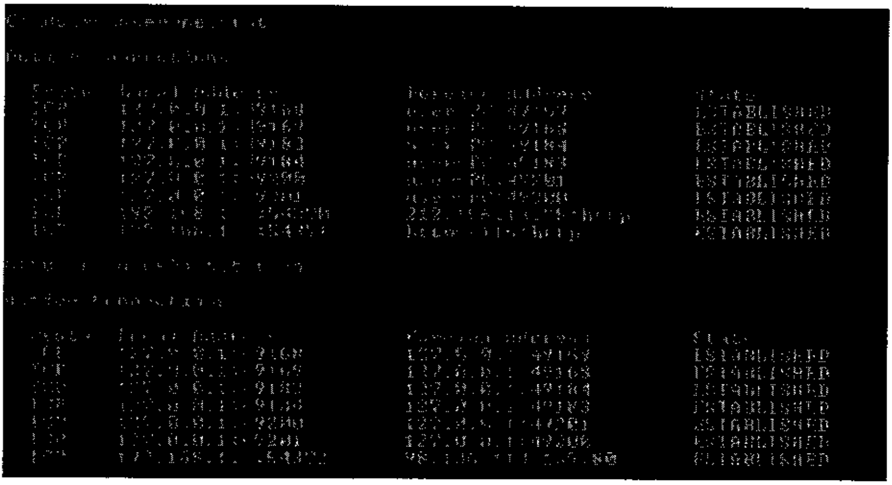

TCP Statistics for IPv4

  Active Opens                        = 8624
  Passive Opens                       = 86
  Failed Connection Attempts          = 527
  Reset Connections                   = 286
  Current Connections                 = 34
  Segments Received                   = 165114
  Segments Sent                       = 154135
  Segments Retransmitted              = 2195
:
UDP Statistics for IPv4

  Datagrams Received    = 5432
  No Ports              = 147
  Receive Errors        = 0
  Datagrams Sent        = 13492
```

: Netstat –n

پس از اجرای فرمان netstat خروجی شما نام دامنه را به جای آدرس IP آن نمایش می دهد. اما با استفاده از این کلید ترکیبی ؛ آدرس IP نمایش داده می شود.تفاوت آنها را در این مثال مشاهده می نمایید.



: Netstat –p

استفاده از این کلید در ترکیب با کلید s- می تواند نتایج خروجی را بر اساس نوع تقاضا به یک پروتکل خاص محدود نماید. این امر باعث می شود در موارد خاص مانند بررسی های امنیتی خروجی محدود تری نمایش داده شود که مشاهده و بررسی آن به مراتب ساده تر باشد.

```
C:\Users\user>netstat -s -p icmp

ICMPv4 Statistics

                            Received    Sent
  Messages                  283         167
  Errors                    0           0
  Destination Unreachable   276         151
  Time Exceeded             3           0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echo Replies              4           0
  Echos                     0           16
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0
  Router Solicitations      0           0
  Router Advertisements     0           0
```

استفاده از nbtstat :

همانگونه قبلا ذکر شد؛ نام های سیستم در NetBIOS در لایه انتقال عمل می نمایند. در بسیاری موارد پروتکل TCP/IP در این سیستم ها مورد استفاده قرار می گیرند. nbtstat وظایف زیر را انجام می دهد :

- آمار مربوط به NetBIOS را در پروتکل TCP/IP پیگیری می نماید.
- جزئیات و مشخصات ارتباطات ورودی و خروجی NetBIOS را در TCP/IP نمایش می دهد.
- عملیات تبدیل اسامی در پروتکل NetBIOS را به آدرس IP انجام می دهد.

خروجی های های مختلف nbtstat :

از آنجا که NetBIOS تنها مختص به سیستم عامل ویندوز است؛ فرمان تنها در سیستم های ویندوزی قابل اجرا می باشد.تمامی کلید های ترکیبی این فرمان نسبت به حروف بزرگ و کوچک حساس هستند. حروف کوچک با نام NetBIOS و حروف بزرگ با آدرس TCP/IP مرتبط هستند. کلید های ترکیبی این فرمان را در این بخش مشاهده می نمایید :

- -A
- -N
- -R
- -S
- -a
- -c
- -r
- -s

: nbtstat –a

این فرمان جدول آدرس های سیستم در پروتکل NetBIOS را نمایش می دهد .در نمایش خروجی این فرمان ، نام؛ نوع اتصال وضعیت اتصال را می توان مشاهده نمود.

- Unique : نمایشگر نام یک سیستم است .
- Group : نمایانگر یک گروه مجازی از کاربران مانند گروه یک گروه کاری یا دامین است .
- Registered : نشان می دهد که این نام در دیگر سیستم ها ثبت شده است .

```
        NetBIOS Remote Machine Name Table

   Name               Type         Status
---------------------------------------------
USER-PC          <00>  UNIQUE      Registered
WORKGROUP        <00>  GROUP       Registered
USER-PC          <20>  UNIQUE      Registered
WORKGROUP        <1E>  GROUP       Registered
WORKGROUP        <1D>  UNIQUE      Registered
..__MSBROWSE__.<01>  GROUP       Registered

MAC Address = 00-  -  -  -  -
```

: nbtstat –A

خروجی فرمان همانند فرمان قبلی است با این تفاوت که در مقابل این فرمان آدرس IP سیستم مورد نظر نوشته می شود و در نهایت خروجی یکسانی تولید می نماید.

```
C:\>nbtstat -A 192.168.1.4
```

nbtstat –c :

این فرمان جدول آدرس مربوط به NetBIOS سیستم کاربر را نمایش می دهد . خروجی این فرمان به این شکل می تواند باشد.

```
Local Area Connection:
Node IpAddress: [192.168.1.4] Scope Id: []

                NetBIOS Remote Cache Name Table

    Name              Type        Host Address    Life [sec]
------------------------------------------------------------
USER-PC        <20>  UNIQUE          192.168.1.4        417
```

- Life : نشان می دهد که این نتایج تا چه مدتی در جدول موجود بوده و پس از آن حذف خواهند شد

nbtstat –n :

این فرمان جدول آدرس مربوط به NetBIOS سیستم کاربر را نمایش می دهد . خروجی این فرمان به خروجی فرمان nbtstat –a شبیه است با این تفاوت که بجای نمایش جدول سیستم دیگر جدول مربوط به سیستم کاربر نمایش داده می شود.

```
          NetBIOS Remote Machine Name Table

    Name               Type         Status
---------------------------------------------
USER-PC          <00>  UNIQUE      Registered
WORKGROUP        <00>  GROUP       Registered
USER-PC          <20>  UNIQUE      Registered
WORKGROUP        <1E>  GROUP       Registered
WORKGROUP        <1D>  UNIQUE      Registered
..__MSBROWSE__.<01>  GROUP       Registered

MAC Address = 00-  -  -  -  -
```

nbtstat –r :

این فرمان پرکاربرد ترین فرمان در هنگام استفاده از آن در پروتکل TCP/IP می باشد.که مشخصات مربوط به تعداد آدرس های تبدیل شده را نمایش می دهد.

```
NetBIOS Names Resolution and Registration Statistics
----------------------------------------------------

Resolved By Broadcast     = 0
Resolved By Name Server   = 0

Registered By Broadcast   = 51
Registered By Name Server = 0
```

این مشخصات به دو بخش تقسیم می شوند:بخش اول که تعداد آدرس های تبدیل شده توسط بسته فراگیر (Broadcast) را نمایش می دهد و بخش دوم تعداد آدرس هایی که توسط سرویس WINSدر سیستم کاربر تبدیل شده باشند را به نمایش قرار می دهد.

: nbtstat –R

این فرمان یک استثنا است زیرا هیچ شباهتی با nbtstat –r ندارد.این فرمان محتویات جدول سیستم را پاک نموده و مقادیر جدید را جایگزین مقادیر قبلی می نماید. نمای کلی این فرمان به این شکل است :

```
C:\>nbtstat –R
```

: nbtstat –S

با کمک این فرمان تمامی اتصالات ورودی و خروجی را می توان مشاهده نمود.در این فرمان آدرس IP سیستم ها نمایش داده می شود. در خروجی این فرمان ورودی یا خروجی بودن اتصال را هم می توان مشخص نمود :

```
                    NetBIOS Connection Table
Local Name             State      In/Out  Remote Host            Input   Output
---------------------------------------------------------------------------------
USER-PC        <00>  Connected     Out        192.168.1.3                    5KB
    4KB
```

: nbtstat –s

با کمک این فرمان تمامی اتصالات ورودی و خروجی را می توان مشاهده نمود.خروجی این سیستم شبیه nbtstat -S می باشد با این تفاوت که درخروجی این فرمان به جای آدرس IP نام سیستم ها نمایش داده می شود.

```
                    NetBIOS Connection Table
Local Name             State      In/Out  Remote Host            Input   Output
---------------------------------------------------------------------------------
USER-PC        <00>  Connected     Out        YOUR-6D39CBC7F0<20>      309KB
    54KB
```

پروتکل انتقال فایل ها FTP :

پروتکل انتقال فایل ها یا FTP پروتکلی بود که برای انتقال داده ها در سیستم های با سیستم عامل یونیکس استفاده می شد.اما امروزه این پروتکل به سیستم فراگیر در بین تمامی سیستم عامل ها برای انتقال داده ها تبدیل شده است . به دلیل قرار داشتن این پروتکل در بسته TCP/IP ، در تمامی نسخه های ویندوز امکان استفاده از این پروتکل وجود دارد.

برای شروع انتقال فرمان FTP را در خط فرمان وارد می نماییم.سپس آدرس مورد نظر برای ورود را با کمک دستور open وارد می نماییم.

```
ftp> open ftp.microsoft.com
```

اگر سرویس FTP فعال و قادر به سرویس دهی باشد پیامی همانند پیام زیر برای شما نمایش داده می شود :

```
C:\Users\user>ftp
ftp> open ftp.microsoft.com
Connected to ftp.microsoft.com.
220 Microsoft FTP Service
User (ftp.microsoft.com:(none)):
```

شما همچنین می توانید فرمان ftp را مستقیم قبل از آدرس مورد نظر استفاده نمایید.این امر به شما اجازه می دهد که مرحله اجرای فرمان و ورود به سرویس دهنده را در یک مرحله انجام دهید. C:\>ftp ftp.microsoft.com

سپس نام کاربری و کلمه عبور معتبر را وارد می نماییم.

برخی سرویس دهندگان اجازه می دهند تا کاربران ناشناس هم بتوانند از این سرویس استفاده نمایند. اما در دیگر سرویس دهنده ها داشتن کلمه کاربری و رمز عبور ضروری است.همچنین بخاطر داشته باشید که کلمه عبور نسبت به حروف کوچک و بزرگ حساس است.

اگر نام کاربری شما صحیح نباشد ؛سیستم پیام خطای شماره ۵۳۰ را نشان می دهد . نمونه آن را در تصویر زیر مشاهده می نمایید.

```
C:\Users\user>ftp
ftp> open ftp.microsoft.com
Connected to ftp.microsoft.com.
220 Microsoft FTP Service
User (ftp.microsoft.com:(none)): test
331 Password required for test.
Password:
530 User cannot log in.
Login failed.
ftp>
```

دریافت توسط FTP :

پس از ورود موفق به سرویس دهنده FTP : شما می توانید داده های مورد نظر خود را جستجو نموده و سپس آنها را دریافت و ذخیره نمایید. محیط کاری این سرویس همانند محیط سیستم عامل DOS می باشد و فاقد گرافیک است . برخی دستورات که در این محیط بکار می روند را در این بخش مشاهده می نمایید:

- Ls : محتویات شاخه را نمایش می دهد. عملکرد آن شبیه دستور DIR در سیستم عامل DOS می باشد.
- Cd : از این فرمان برای تغییر شاخه استفاده می شود که همانند دستور CD در سیستم عامل DOS می باشد.
- Pwd :آدرس و مشخصات شاخه فعلی را نمایش می دهد. زمانی کاربرد دارد که به دلیل تغییرات زیاد؛ آدرس فعلی فراموش شده باشد
- Lcd : محل ذخیره شدن داده های دریافتی در سیستم کاربر را تغییر می دهد.

پس از جستجو و یافتن داده های مورد نظر ؛ حال نوبت به دریافت آنها می رسد. برای دریافت از فرمان get استفاده می شود . با این فرمان فایل testsrv.exe از روی سرور دریافت می شود

```
ftp> get testsrv.exe
```

متاسفانه در هنگام ذخیره سازی ؛هیچگونه آمار و اطلاعاتی در مورد مراحل ذخیره سازی به کاربر اعلام نمی شود. تنها پس از تکمیل انتقال ؛ پیام نهایی به کاربر اعلام می گردد.

استفاده ازفرمان ping :

```
C:\Users\user>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

از این فرمان برای برسی اتصال به شبکه استفاده می شود . در این فرمان پس از فرمان Ping آدرس IP مورد نظر برای انجام پینگ را اضافه می نماییم.

استفاده از کلید های ترکیبی ؛ خروجی های زیر را تولید می نماید :

- -t : آدرس مورد نظر را بدون وقفه پینگ می نماید.

- ❖ -n : تعداد دفعات انجام پینگ را مشخص می نماید.
- ❖ -w : میزان فاصله بین انجام هر اجرای فرمان پینگ
- ❖ -l : سایز بافر را مشخص می نماید
- ❖ -4 : سیستم را مجبور می نماید که از نسخه ۴ IP استفاده نماید.

استفاده ازفرمان های winipcfg ؛ ipconfig و ifconfig :

درنسخه های مختلف ویندوز ابزاری برای نمایش وضعیت و تنظیمات TCP/IP وجود دارد که در نسخه های مختلف با هم تفاوت دارند. در این بخش با آنها آشنا می شویم :

استفاده از ابزار ipconfig :

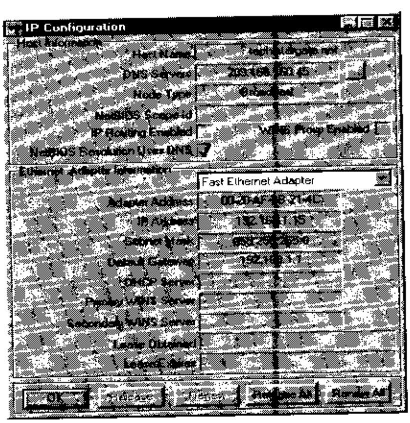
همانگونه که می دانید نسخه NT ویندوز از ابتدا برای سازگاری با سیستم عامل یونیکس طراحی شده بود؛ از این رو برخی فرمانهای یونیکس قابل اجرا در سیستم عامل ویندوز هستند که برخی از آنها بدین شرح هستند :

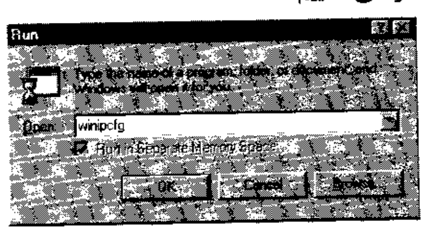
- ❖ ftp
- ❖ ping
- ❖ tracert
- ❖ ipconfig

عملکرد فرمان ipconfig دقیقا همانند عملکرد winipcfg در نسخه های ۹۸/۹۵ ویندوز می باشد

استفاده ازفرمان winipcfg :

ابزار winipcfg برای نمایش و با اعمال تغییرات در نسخه های ۹۸/۹۵ ویندوز استفاده می شود بدین منظور این فرمان را در ویندوز اجرا می نماییم.





در خروجی این ابزار کاربردی ؛ شما تمامی اطلاعات مربوط به تنظیمات TCP/IP و آدرس اختصاص یافته شده توسط DHCP را نیز می توانید مشاهده نمایید.

استفاده از ابزار ipconfig :

همانگونه که می دانید نسخه NT ویندوز از ابتدا برای سازگاری با سیستم عامل یونیکس طراحی شده بود ؛ از این رو برخی فرمانهای یونیکس قابل اجرا در سیستم عامل ویندوز هستند که برخی از آنها بدین شرح هستند :

- ftp
- ping
- tracert
- ipconfig

عملکرد فرمان ipconfig دقیقا همانند عملکرد winipcfg در نسخه های ۹۸/۹۵ ویندوز می باشد. خروجی این فرمان به این شکل می باشد :

```
Windows IP Configuration

 Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::24c4:ec67:c9a5:8a80%10
    IPv4 Address. . . . . . . . . . . : 192.168.1.4
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 192.168.1.1
```

همانگونه که مشاهده می کنید خروجی این فرمان همانند winipcfg می باشد با این تفاوت که آدرس فیزیکی نمایش داده نمی شود. با استفاده از فرمان ipconfig/all می توانیم خروجی کاملی داشته باشیم. با دستور ipconfig/release آدرس دریافت شده از سرور DHCP حذف می شود و با فرمان ipconfig/renew تمامی آدرس های دریافت شده از سرور حذف می شود و سپس آدرس جدی از سرور DHCP در یافت می شود

استفاده از ابزار ifconfig :

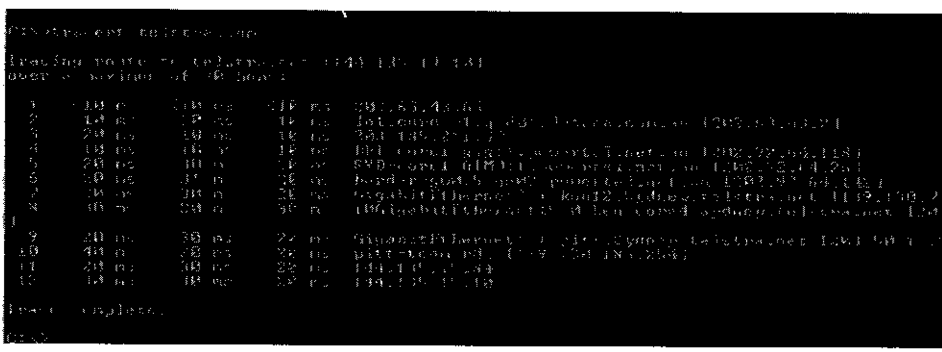
ابزاری که در سیستم عامل لینوکس و یونیکس استفاده می شود ifconfig می باشد که خروجی آن شبیه خروجی ipconfig می باشد . اگرچه خروجی آنها یکسان می باشد اما تفاوت اصلی در این است که فرمان ipconfig تمامی تنظیمات TCP/IP در سیستم را نمایش می دهد اما با ifconfig تنظیمات مربوط به یک کارت شبکه خاص را می توان نمایش داد. در خروجی زیر تنظیمات یک کارت شبکه را مشاهده می نمایید :

```
[root@monarch ~]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0D:88:2D:2B:34
          inet addr:192.168.3.10  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::20d:88ff:fe2d:2b34/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:2432 (2.3 KiB)
          Interrupt:11 Base address:0xd400
```

در این خروجی آدرس فیزیکی ؛آدرس IP ؛ و حجم ارسال و دریافت همچنین مشکلات ارسال و دریافت داده ها را می توان مشاهده نمود.

استفاده از ابزار tracert :

با این ابزار می توان مسیر داده ها ی ارسال شده تا مقصد نهایی آنها را مشاهده نمود. این ابزار برای مشخص نمودن مشکلات در ارسال داده ها بسیار کاربرد دارد. در خروجی این فرمان تمامی مسیر طی شده توسط داده ها را می توانید مشاهده نموده و در صورت بروز اشکال در ارسال نقطه ایجاد مشکل را مشخص و آن را برطرف نمود.



استفاده از ابزار Telnet :

این ابزار در اصل برای ایجاد یک ارتباط میان کاربر و سرور هایی با سیستم عامل یونیکس طراحی از طریق ترمینال توسعه یافته بود. امروزه این ابزار در سیستم عامل ویندوز با همان کاربرد وجود دارد. برای برقراری این ارتباط از پورت شماره ۲۳ در پروتکل TCP استفاده می شود.

البته شما می توانید از این ابزار برای برسی عملکرد پورت ها نیز استفاده نمایید بدین صورت که شما می توانید با تمامی پورت ها ارتباط برقرار نمایید. در صورت برقراری ارتباط ؛عملکرد آن پورت صحیح می باشد.

برای برقراری ارتباط ؛ شکل عمومی آن به این شکل است که با پارامتر های زیر می توان خروجی های مختلفی تولید نمود :

```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> ?

Commands may be abbreviated. Supported commands are:

c    - close                    close current connection
d    - display                  display operating parameters
o    - open hostname [port]     connect to hostname (default port 23).
q    - quit                     exit telnet
set  - set                      set options (type 'set ?' for a list)
sen  - send                     send strings to server
st   - status                   print status information
u    - unset                    unset options (type 'unset ?' for a list)
?/h  - help                     print help information
Microsoft Telnet> telnet www.yoursite.com 80_
```

Close : ارتباط برقرار شده را قطع می نماید.

Open :ارتباط مورد نظر را برقرار می نماید.

Exit : از ابزار telnet خارج می شود.

در صورت برقراری موفق ارتباط؛ پیامی را مبنی بر موفق بودن ارتباط مشاهده نمی نمایید اما درصورت بروز اشکال در ارتباط شما پیام وجود اشکال را مشاهده خواهید نمود.

استفاده از ابزار nslookup :

برای اتصال سیستم به اینترنت ؛ تنظیم سرویس DNS بسیار مهم و ضروری است. این سرویس وظیفه تبدیل نام دامنه اینترنتی را به آدرس IP آن برعهده دارد. هنگام تنظیم این سرویس بسیار مهم است که شما بتوانید بررسی کنید که آدرس وارد شده به درستی تبدیل شده یا خیر.

برای این منظور از ابزار nslookup استفاده می نماییم.این ابزار به شما نمایش می دهد که چه نامی به چه آدرس IP تبدیل شده است.

در سیستم عامل یونیکس ابزار dig همین عمل را انجام می دهد.ابزار dig هم در خط فرمان اجرا شده و نتیجه ای همانند ابزار nslookup تولید می نماید.

در نسخه های ویندوز NT و پس از آن این فرمان قابل اجرا می باشد. البته در نسخه های ۹۸/۹۵ ویندوز هم از خط فرمان ویندوز اجرا می گردد.

```
C:\Users\user>nslookup
Default Server:  vnsc-pri-dsl.genuity.net
Address:  4.2.2.4

>
```

برای تبدیل نام دامنه به آدرس IP ؛ نام دامنه را وارد نموده و اطلاعات مربوط به آدرس IP آن از سرویس دهنده DNS مشخص شده ؛ دریافت و نمایش داده می شود .

```
> yahoo.com
Server:  vnsc-pri-dsl.genuity.net
Address:  4.2.2.4

Non-authoritative answer:
Name:    yahoo.com
Addresses:  69.147.114.224
          209.131.36.159
          209.191.93.53

>
```

در این خروجی مشخص می شود که اطلاعات از سرویس دهنده ای با آدرس : 4.2.2.4 دریافت شده و دامنه yahoo.com دارای آدرس های IP نمایش داده شده می باشد.

جمع بندی:

در این بخش شما:

- ❖ درخصوص تنظیمات و کلید های ترکیبی ابزار های nbtstat,netstat , arp مطالب مهمی آموختید. این ابزارهای کاربردی برای رفع مشکل شبکه بسیار سودمند هستند.
- ❖ نحوه بررسی و شناسایی مشکلات در شبکه ها را با کمک ابزار ping و tracert آموختید.
- ❖ با عملکرد فرمان ping و نقش آن در شناسایی مشکلات در شبکه آشنا شدید.
- ❖ با عملکرد فرمان tracert در شبکه آشنا شدید.
- ❖ در خصوص پروتکل انتقال داده ها یا FTP مطالب مفیدی آموختیتد .
- ❖ با عملکرد ها و تفاوت های ipconfig ؛ ifconfig وwinipcfg آشنا شده و عملکرد های تکمیلی آنها را فرا گرفتید.
- ❖ باعملکردها و تفاوت های ابزار های سرویس DNS که nslookup و dig هستند آشنا شدید.

سوالات ارزیابی برای آزمون Network+ :

۱ –کدامیک از این ابزار برای سنجش سلامت و عملکرد سرور یا سیستم بکار می رود.

الف) FTP

ب) Telnet

ج) ping

د) netstat

۲-کدامیک از این ابزار برای نمایش آدرس فیزیکی و آدرس IP سیستم بکار می رود.

الف) ipconfig

ب) winipcfg

ج) tracert

د) telnet

۳-خروجی زیر مربوط به کدامیک از ابزار TCP/IP است.

```
Pinging 4.2.2.4 with 32 bytes of data:
Reply from 4.2.2.4: bytes=32 time=445ms TTL=49
Reply from 4.2.2.4: bytes=32 time=423ms TTL=49
Reply from 4.2.2.4: bytes=32 time=324ms TTL=49
Reply from 4.2.2.4: bytes=32 time=377ms TTL=49
```

الف) winipcfg

ب) tracert

ج) Ping

د) wins

۴- کدام ابزار برای سنجش سلامت کارت شبکه مورد استفاده قرار می گیرد. (تمامی موارد صحیح را مشخص نمایید)

الف) tracert 127.0.0.1

ب) test 127.0.0.1

ج) ping 127.0.0.1

د) ping localhost

۵- با کدامیک از این فرامین می توان فایل را با کمک پروتکل FTP دریافت نمود. (تمامی موارد صحیح را مشخص نمایید)

الف) get

ب) down

ج) lpd

د) lcd

۶- خروجی زیر مربوط به کدامیک از ابزار زیراست .

```
  1     2 ms     4 ms     3 ms  192.168.15.1
  2     2 ms     2 ms     2 ms  mygateway1.ar7 [192.168.1.1]
  3   180 ms    14 ms    19 ms  188.158.8.1
  4   267 ms    42 ms    32 ms  89.165.0.248
  5   161 ms   213 ms   270 ms  89.165.3.33
  6   121 ms    79 ms    23 ms  89.165.3.129
  7     *        *       20 ms  195.146.63.253
  8   295 ms   274 ms   282 ms  ldn-b1-link.telia.net [213.248.76.5]
  9   410 ms   245 ms   289 ms  ldn-bb1-link.telia.net [80.91.248.90]
 10   282 ms   392 ms     *     ldn-b5-link.telia.net [80.91.247.90]
 11   300 ms   346 ms   381 ms  globalcrossing-ic-135890-ldn-b5.c.telia.net [213
.248.81.74]
 12   328 ms   495 ms     *     Yahoo.TenGigabitEthernet3-4.ar4.DAL2.gblx.net [6
4.211.211.130]
 13     *      433 ms   407 ms  216.115.104.107
 14   413 ms   536 ms   538 ms  te-8-2.fab2-a-gdc.mud.yahoo.com [209.191.78.157]

 15   513 ms     *      336 ms  UNKNOWN-209-191-78-175.yahoo.com [209.191.78.175
]
 16   448 ms     *      374 ms  yahoo.com [209.191.93.53]
```

الف)netstat

ب) ping

ج) nbtstst

د) tracert

۷-کدام کلید در کنار فرمان ipconfig خروجی کامل را نمایش می دهد .

الف)a/

ب) release/

ج) all/

د) full/

۸-کدامیک از فرامین زیر برای نمایش تنظیمات TCP/IP در ویندوز ۲۰۰۰ بکار می رود. (تمامی موارد صحیح را مشخص نمایید)

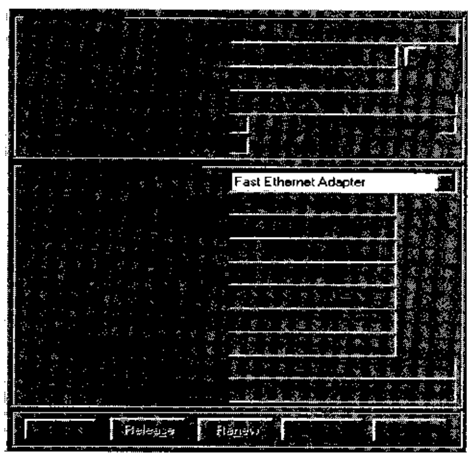
الف) arp

ب) winipconfig
ج) ipconfig
د) winipcfg

۹- شما مدیر یک شبکه هستید . یکی از کاربران از کیفیت پایین اینترنت خود شکایت دارد. پس از بررسی مشخص می شود که مشکل مربوط به یکی از مسیر یاب های بین راه است. با کمک کدام ابزار می توان مشخص کرد که مشکل از کدام مسیر یاب است.

الف) telnet
ب) tracert
ج) ping
د) ipconfig

۱۰-خروجی زیر مربروط به کدام فرمان است.



الف) ipconfig
ب) winipcfg
ج) tracert
د) arp

پاسخ به سوالات این بخش

۱ - ج

ابزار ping برای سنجش سلامت و عملکرد سرور یا سیستم بکار می رود.

۲ - الف، ب

ابزار winipcfg وipconfig برای نمایش آدرس فیزیکی و آدرس IP بکار می روند.

۳ - ج

با توجه به توضیحات این فصل خروجی مربوط به فرمان Ping است.

۴ - ب

فرمانی با ساختار test 127.0.0.1 وجود ندارد.

۵ - الف

با فرمان Get می توان فایل را با کمک پروتکل FTP دریافت نمود.

۶ - د

این خروجی مربوط به فرمان tracert می باشد.

۷ - ج

با کلید all/ تمام تنظیمات نمایش داده می شو و release/ مربوط به DHCP می باشد.a/ و full/ وجود ندارد.

۸ - ج

Winipcfg تنها در نسخه های ۹۵و ۹۸ کاربرد دارد.

۹ - ب

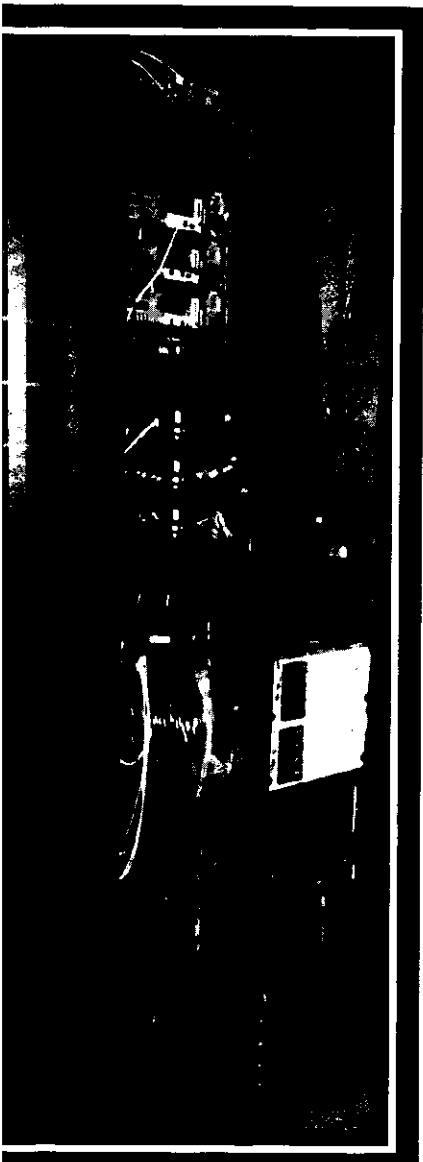
با کمک این فرمان می توان تمام مسیر بین مبدا تا مقصد را بررسی نموده و اشکالات احتمالی در تجهیزات بین راد را تشخیص داد.

۱۰ ـ ب

خروجی گرافیکی مربوط به فرمان winipcfg می باشد.

فصل پنجم

سیستم عامل های شبکه



شما در این فصل با این مفاهیم آشنا خواهید شد:

۵-۱ شناسایی نقات قوت و ضعف سیستم عامل های شبکه مانند:
سازگاری؛ اشتراک قراردادن چاپگر و فایل ها ؛امنیت ؛پشتیبانی از نرم افزار ها و نحوه تصدیق ورود کاربران در سیستم های عامل زیر :

- UNIX/Linux/Mac OS X Server
- NetWare
- windows
- AppleShare IP (Internet Protocol)

فصل پنجم- سیستم عامل های شبکه

مقدمه:

هرشبکه امروزی ؛ نرم افزاری داردکه از آن برای مدیریت برمنابع شبکه بکار گرفته می شود.این نرم افزار بر روی یک سیستم قوی که آن را سیستم عامل شبکه یا (NOS(Network Operating System می گویند ، نصب شده و عملیات مدیریت شبکه را برعهده می گیرد که بدون شک یکی از مهمترین اجزای شبکه های امروزی می باشد.

در این بخش به بررسی متداولترین سیستم های عامل شبکه می پردازیم:

- Microsoft Windows
- Novell Net Ware
- Unix / Linux
- Macintosh

NetWare توسط شرکت Novell تهیه شده است که آن را می توان اولین سیستم عامل شبکه تجاری دانست. ویندوز هم در سال ۱۹۹۳ توسط مایکروسافت تولید شد و توانست سهم عمده ای از بازار را بدست آورد. یونیکس قدیمی ترین سیستم عامل شبکه است که با کمک سیستم عامل لینوکس که برگرفته از این سیستم عامل است سعی در جذب کاربران دارد. لینوکس سهم عمده ای در شبکه اینترنت دارد زیرا بخشی از این شبکه عظیم براین بستر قرار گرفته است. آخرین سیستم عامل که سهمی بسیار اندک را دارد AppleShare IP است که در سیستم عامل Mac OS X شرکت مکینتاش استفاده می شود.

مایکرو سافت ویندوز :



با کمک گرفتن از جلوه های گرافیکی استفاده شده در نسخه های ویندوز و نحوه مدیریت بسیار آسان آن ؛ ویندوز امروزه مهمترین سیستم عامل در دنیای شبکه می باشد.

در سال ۱۹۹۳ مایکروسافت نسخه ۳.۱ ویندوز را معرفی نمود که اولین سیستم عامل شبکه این شرکت بود. پس از آن در سال۱۹۹۴ نسخه بعدی یعنی ۳.۵۱ معرفی گردید. اما هنوز تا رسیدن به نسخه های امروزی راهی طولانی باقی مانده بود. در این نسخه ها تنها امکانات مدیریتی به نسخه ۳.۱ ویندوز اضافه شده بود که ترکیبی از زیبایی و کارایی در آن دوران بودند.

با همه گیر شدن نسخه های NT ویندوز؛ این سیستم عامل بزودی توانست که جای سیستم عامل های دیگر مانند NetWare و نسخه های متنوع لینوکس را در بازار شبکه بگیرد.

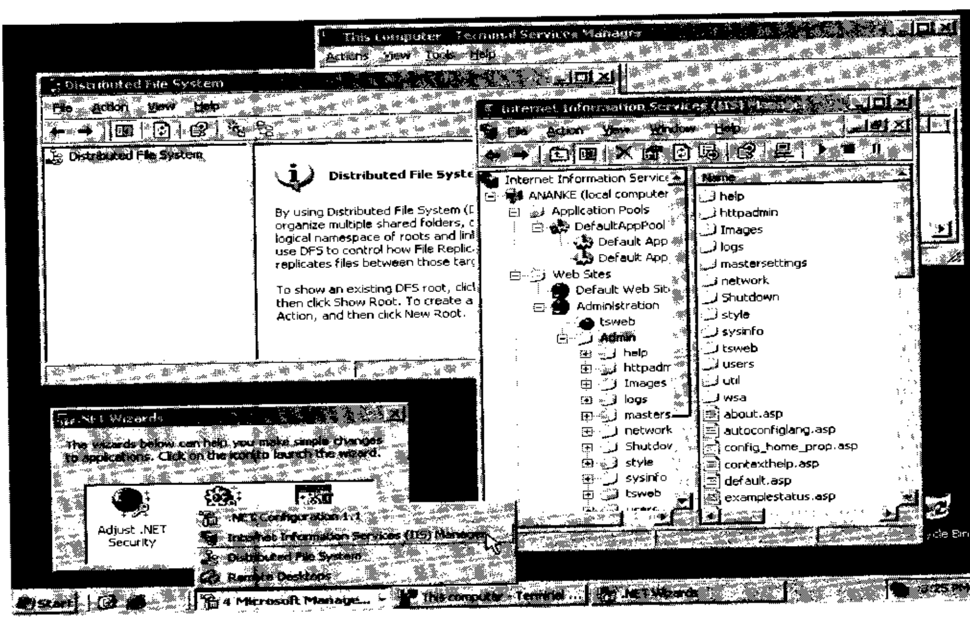
نسخه های بعدی که ۲۰۰۰ ؛ ۲۰۰۳ و ۲۰۰۸ هستند به سرعت به سیستم عامل بدون رقیب در بازار شبکه تبدیل شدند.در این بخش ما با امکانات و مشخصات این سیستم عامل بیشتر آشنا می شویم :

امکانات :

این سیستم عامل انتخاب اول و آخر تولید کنندگان نرم افزار است زیرا تمامی نسخه های ویندوز شبیه هم هستند و براحتی می توان نرم افزار های متفاوتی برای تمامی نسخه های ویندوز تهیه نمود. نکته مهم دیگر این است که در هنگام نصب این سیستم عامل ؛تمامی سرویس های شبکه را براحتی می توان از لوح فشرده این سیستم عامل انتخاب نموده و نصب کرد.و اما مهم ترین دلیل این است به دلیل شباهت با نسخه های کاربر پسند ویندوز مدیران شبکه وقت بسیار اندکی را باید صرف آموزش و یادگیری این سیستم عامل نمایند.

رابط کاربری ویندوز:

محیط گرافیکی نسخه شبکه همانند نسخه های دیگر ویندوز است از این رو محیط آن برای اکثر کاربران محیطی آشنا و دوست داشتنی است. و تمامی سرویس های شبکه را می تواند با رابط گرافیکی اجرا نماید.



پشتیبانی از نرم افزار های جانبی :

همانگونه که ذکر کردیم با همه گیر شدن سریع ویندوز؛ بسیاری از شرکت های نرم افزاری اقدام به تهیه نرم افزار های کاربردی مختلفی برای این سیستم عامل نمودند که هرکدام از آنها می توانند مدیران شبکه را در وظایفشان یاری نمایند.یکی از محاسن تهیه نرم افزار برای ویندوز امکان استفاده از این نرم افزار ها در هر دو نسخه شبکه و کاربری ویندوز است. از این رو شرکت ها بیشتر راغب هستند که برای این سیستم عامل نرم افزار تهیه کنند تا سیستم عامل های دیگر شبکه.

پشتیبانی از کاربران :

علاوه بر اینکه سیستم عامل شبکه ویندوز از تمامی نسخه های ویندوز پشتیبانی می نماید بلکه با اضافه کردن برخی نرم افزارهای افزودنی می تواند از کاربران سیستم عامل های لینوکس و مکینتاش هم پشتیبانی نماید. البته پشتیبانی از ویندوز کامل و همه جانبه بوده ولی پشتیبانی از کاربران سیستم عامل های دیگر محدود و تحت شرایط خاصی انجام می پذیرد.

قابلیت سازگاری با سیستم های دیگر :

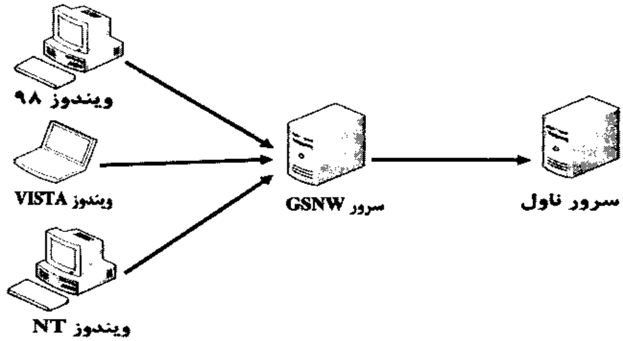
با توجه به گسترش سیستم های عامل و تنوع آنها ؛ یک سیستم عامل فراگیر می بایست امکان برقرای ارتباط با تمامی سیستم عامل های کاربران را داشته باشد.امروزه این قابلیت با افزودن برخی امکانات به ویندوز فراهم شده است.

یکی از این قابلت ها؛امکان برقرای ارتباط سرویس های یونیکس با سیستم عامل ویندوز است برای این منظور یک زیر سیستم در سیستم عامل با نام Interix باید ایجاد شود که اجرای فرامین برای شبکه های مبتنی بر یونیکس در این بخش اجرا می گردد.به علاوه پس از معرفی سیستم عامل NT مایکروسافت می بایست که تعامل با سیستم عامل شرکت ناول یعنی NetWare ایجاد گردد. در زمانی که ویندوز نسخه ۳.۱۱ را در سال ۱۹۹۳ معرفی نمود؛تقریبا ۷۵ درصد بازار شبکه در اختیار شرکت ناول بود ؛از این رو سیستم عامل جدید می بایست مطابق با نیاز روز پیکر بندی می شد. برای این منظور سرویس هایی به ویندوز اضافه گردید.این سرویس ها عبارتند از :

- درگاه خروجی برای سیستم عامل ناول (GSNW)
- سرویس پشتیبانی برای کاربران سیستم عامل ناول (CSNW)
- سرویس اشتراک قرار دادن چاپگر و فایل برای کاربران سیستم عامل ناول (FPNW)

درگاه خروجی برای سیستم عامل ناول (GSNW):

وظیفه این سرویس تبدیل درخواست های دسترسی به منابع ویندوز به درخواست های سیستم عامل ناول می باشد. این سرویس می تواند دسترسی کاربران شبکه ویندوز را از طریق این سرویس به منابع شبکه های ناول برقرار نماید.



سرویس پشتیبانی برای کاربران سیستم عامل ناول (CSNW):

این سرویس را می توان آسانترین سرویس ارتباط با سیستم عامل ناول دانست ؛ اما اجرای آن روی سیستم های شبکه بسیار سخت و وقت گیر است.زیرا می بایست بر روی سیستم تمامی کاربرانی که قصد استفاده از منابع سیستم عامل ناول هستند نصب گردد. علاوه بر این به ازای هر سیستم باید مجوز ورود و استفاده از منابع بر روی سرور تعریف گردد.

سرویس اشتراک قرار دادن چاپگر و فایل برای کاربران سیستم عامل ناول (FPNW) :

این سرویس برای ایجاد اشتراک فایل و چاپگر بر روی سرور ویندوز جهت استفاده کاربران سیستم عامل ناول مورد استفاده قرار می گیرد.با اجرای این سرویس؛ سرور مورد نظر همانند یک سرور با سیستم عامل ناول عمل می نماید. این سرویس زمانی مورد استفاده قرار می گیرد که شما در سیستمتان تعدادی سرور ویندوز و تعدادی هم سرور ناول همزمان مشغول به کار باشند.

سنجش اعتبار:

بعد از ویندوز ۲۰۰۰ ،تمامی محصولات ویندوز امکان استفاده از کربروس (Kerberos) را برای سنجش اعتبار کاربران فراهم نموده است . علاوه بر این امکان سنجش اعتبارکاربران با کمک ابزار مدیریت کاربران شبکه ویندوز با نام Active Directory (AD) که معادل سرویس Novell Directory (ND) می باشد هم امکان پذیر

می باشد.در این روش هنگام ورود کاربر ؛ نام کاربری و کلمه عبور از بانک اطلاعاتی AD مورد بررسی قرار می گیرد.

کربروس یک پروتکل اعتبارسنجی در شبکه است.در این روش برای هر کاربری که اعتبارش با موفقیت مورد تایید قرار گیرد یک کلید تولید می شود که این کلید به همراه تمامی بسته های ارسالی کاربر در شبکه ارسال می شود تاهویت فرستنده بسته هارا مشخص نماید.

اشتراک قراردادن فایل و چاپگر :

این سرویس ویندوز پاسخگوی تمامی نیاز های کاربران می باشد. با راه اندازی این سرویس در شبکه های کوچک و متوسط؛می توان اشتراک قرار دادن فایل و چاپگر بر روی شبکه را برای کاربران متعدد شبکه ممکن ساخت.یکی از مزایای این سرویس آشنایی کاربران با محیط و نحوه کار با ویندوز است .

برای این کار فایل های مورد نظرجهت اشتراک را در سیستم ذخیره نموده و مجوز اشتراک آنها بر روی شبکه برای دیگر کاربران را صادر می نماییم. بسته به تدابیر امنیتی که بر این اشتراک تنظیم شده اند دیگر کاربران شبکه اجازه مشاهده یا اعمال تغییرات بر روی این فایل ها را خواهند داشت.

مطابق با همین روش ؛ برای اشتراک چاپگر بر روی شبکه عمل می نماییم یعنی چاپگر روی سرور نصب شده و مجوز اشتراک آن صادر می شود. در اولین ارتباط با چاپگر ؛ نرم افزار مربوط به آن بصورت خودکار بر روی بر روی رایانه کاربر نصب می شود و پس ازاین مرحله کاربر شبکه می تواند از این چاپگر استفاده نماید.

پشتیبانی از نرم افزارهای کاربردی :

در زمینه پشتیبانی از نرم افزارهای کاربردی ویندوز بسیار خوش درخشیده است. بدون شک ویندوز را می توان بهترین سیستم عامل از نظر پشتیبانی توسعه دهندگان نرم افزار دانست.تقریبا هر نرم افزاری که بر روی نسخه های VISTA /XP/۹۸ ویندوزنصب می شود را می توان برروی نسخه ۲۰۰۳ هم نصب نمود ازطرفی با یکسان بودن محیط کاربری نسخه های ویندوز؛کار با این سیستم عامل را برای کاربران بسیار آسان و دوست داشتنی نموده است.

امنیت :

علیرغم تمامی محاسن این سیستم عامل که در این فصل ذکر کردیم ؛ امنیت این سیستم عامل در حد انتظار نیست. از این رو اکثر بسته های به روزرسانی برای نسخه های سرور ویندوز؛ وصله های امنیتی هستند. این سیستم

در مقابل حملاتی اینترنتی بسیار آسیب پذیر است و به دلیل سهولت کاربرد درمقابل نفوذگران شبکه هم آسیب پذیری بیشتری از خود نشان می دهد و همیشه باید به روز باشد.

برای بدست گرفتن بازار ؛مایکروسافت ابتدا نسخه نرم افزار مورد نظر را وارد بازار می نماید و سپس سعی در رفع مشکلات بوجود آمده از طریق وصله های افزودنی می نماید این روش باعث ایجاد مشکلات بسیاری برای کاربران می شود اما همه این موارد چیزی از محبوبیت این سیستم عامل کم نمی کند.

البته باید این نکته را ذکر نمود که این مسایل به این معنی نیست که ویندوز سیستم عامل امنی نیست بلکه برقراری امنیت این سیستم عامل نیاز به کار بیشتری دارد.شما می بایست همیشه مطمئن باشید که سیستم عامل شما بروز بوده و تمامی بسته های افزودنی شرکت مایکروسافت بر روی آن نصب شده است. در این صورت سیستم عامل شما از نظر امنیتی با دیگر سیستم عامل ها در یک وضعیت قرار دارد.

Novell NetWare :

این سیستم عامل یکی از مهمترین سیستم عامل ها در بازار شبکه است.این سیستم عامل محدودیتی از نظر تعداد کاربران و حجم شبکه مورد استفاده ندارد. اکثر شبکه ها با مقیاس بزرگ از این سیستم عامل استفاده می نمایند.

در این بخش ما به اختصار در مورد برخی موارد کلیدی در مورد این سیستم عامل اشاره می نماییم. برای آگاهی از جدیدترین تغییرات این سیستم عامل به آدرس www.novell.com مراجعه نمایید.

امکانات :

این سیستم عامل در بین شبکه های بزرگ که معمولا بیشتر از ۲۰ سرور دارند به دلیل قابلیت مدیریت متمرکز سرور ها و کاربران شبکه مورد استفاده قرار می گیرد.برخی امکانات این سیستم عامل که در نسخه ۴ به بعد آن وجود دارد به این شرح است :

- سیستم مدیریت کاربران و سیستم ها
- حداقل امکانات سخت افزاری برای اجرا مورد نیاز است.
- پشتیبانی از اکثر سازندگان سخت افزار
- پشتیبانی از نرم افزار ها
- قابلیت سازگاری با سیستم های دیگر

سیستم عامل ناول را می توان بهترین گزینه برای اشتراک قراردادن فایل و چاپگر ومدیریت کاربران دانست. امروزه با استفاده فراوان از تکنولوژی جاوا در این سیستم عامل ؛ به آرامی خود را به عنوان سرور کاربردی برای نرم افزار های کاربردی تحت جاوا معرفی کرده است .

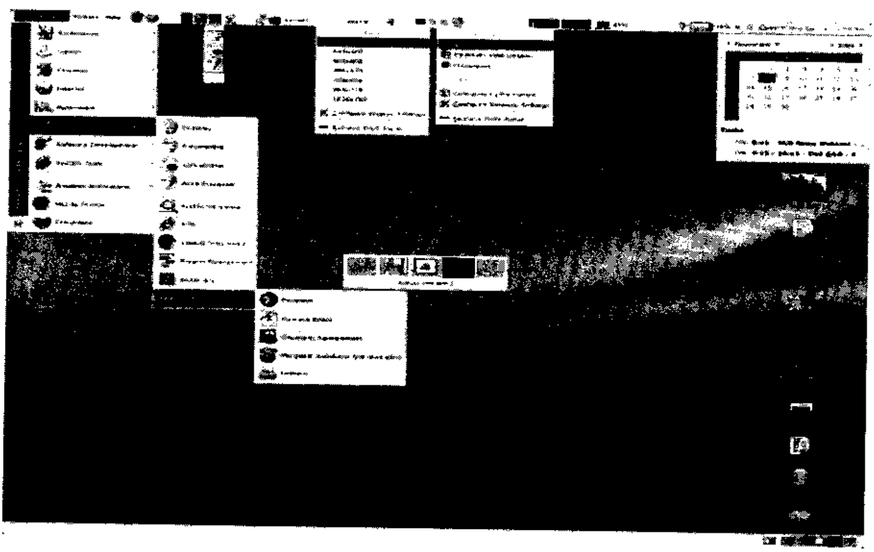
پشتیبانی از کاربران :

سیستم عامل ناول بخش مربوط به ارتباط با سیستم عامل های دیگر را توسعه داده است تا بتواند سیستم عامل های بیشتری را پشتیبانی نماید و آنها بتوانند از امکانات این سرور ها بهره مند گردند.

برای این منظور کاربران سیستم عامل های دیگر برای ارتباط با این سیستم عامل باید نرم افزار مربوط به اتصال با سرورهای ناول که توسط تولید کننده همان سیستم عامل طراحی شده است را بر روی رایانه خود نصب نمایند. البته ناول برای برخی سیستم عامل ها نظیر یونیکس این نرم افزار ارتباطی را خود تهیه کرده است. البته برخی توسعه دهندگان لینوکس امروزه از این نرم افزار استفاده ننموده و خود این نرم افزار ارتباطی را تهیه نموده و به سیستم عامل های خود افزوده اند.

رابط کاربری :

در این تصویر ؛ رابط گرافیکی سیستم عامل NetWare که در محیط سیستم عامل لینوکس اجرا شده است را مشاهده می نماییم.



قابلیت سازگاری با سیستم های دیگر :

سیستم عامل NetWare بسیار انعطاف پذیر بوده و تقریبا با اکثر سیستم عامل های شبکه سازگار است. برخی از این سیستم عامل ها عبارتند از :

- ویندوز نسخه های ۹۸/۹۵/ XP/ NT/ Vista/Server /Me
- Mac OS
- یونیکس
- OS/400
- OS/2
- VMS

هرگاه کاربر یکی از این سیستم عامل ها بخواهد با سیستم عامل NetWare ارتباط برقرار نماید ؛ سرور مورد نظر بصورت مجازی همانند یک سرور از همان سیستم عامل عمل می نماید تا کاربر بتواند از امکانات آن استفاده نماید.

سنجش اعتبار کاربران:

در این مرحله که توسط سیستم عامل انجام می گیرد ؛در واقع تعیین هویت کاربری است که درخواست ورود به شبکه و با استفاده از منابع شبکه را دارد. تمامی نسخه های ناول پس از نسخه ۴ دارای سیستم مدیریت کاربران یا NDS می باشد. این یکی از امکانات سیستم عامل های شبکه است که با مدیریت منابع و کاربران امکان دسترسی به منابع شبکه را فراهم می آورد.

بطور کلی ۳ نوع سیستم مدیریت کاربران وجود دارد:

بایندری :

این سیستم با امکاناتی بسیار ساده وپیش پا افتاده است ؛ بانک اطلاعاتی کاربران که اطلاعات مربوط به گروه ها و اطلاعات امنیتی کاربران را در سرور ذخیره می نماید. این سیستم در نسخه های قبل از نسخه ۴ وجود داشت.

سیستم مدیریت کاربران ناول NDS :

در این سیستم شما بر اساس سلسله مراتب ؛ دسترسی به تمامی اعضا شبکه خواهید داشت. که البته این امکان در نسخه قبل از ۴ موجود نیست. نامگزاری اجزای شبکه بر اساس استاندارد X.500 انجام می گیرد. بانک اطلاعاتی در این سیستم دایرکتوری نام دارد. البته نباید آن را با مفهوم شاخه در سیستم عامل DOS اشتباه گرفت.

برای سهولت در یافتن یکی از اجزا شبکه در این سیستم؛ تمامی اجزا شبکه دارای یک مشخصه هستند که تمامی اطلاعات مورد نیاز را در خود ذخیره می نماید این اطلاعات را value می نامند

در این سیستم اطلاعات کاربران در سرور ها ذخیره می شود و هر سرور می داند که سرور دیگری که اطلاعات کاربران را ذخیره می کند در کجا قرار دارد تا در صورت لزوم اطلاعات را از آن دریافت کند پس این سیتم را می توان شبکه محور دانست.

EDirectory :

این سیستم در واقع افزونه ای برای NDS می باشد با این افزونه سیستم های مدیریت کاربران روی بستر شبکه اینترنت به هم متصل شده و یک سیستم یکپارچه ایجاد نمایند. نسخه های امروزی NDS همگی دارای دایرکتوری الکترونیکی یا EDirectory هستند.

مزیت عمده NDS بر بایندری را می توان به تفاوت ساختاری آن دانست. در NDS ساختار کلی و سلسله مراتبی همانند یک شاخه های یک درخت وجود دارد ؛از این رو آن را ساختار درختی یا Treeمی گویند. البته این ساختار منطقی است نه فیزیکی.

در این حالت تمامی اجزا شبکه مانند کاربران ؛ سرور ها ؛ چاپگر ها و دیگر اجزا شبکه در یک ساختار منظم مشخص شده اند.از سوی دیگر در بایندری تنها اطلاعات کاربرانی که در آن بخش شبکه وجود دارند ذخیره می شود حال آنکه NDS را می توان یک سیستم یکپارچه سراسری مرکزی شبکه دانست اما بایندری تنها یک سرور مرکزی است .

اشتراک قراردادن فایل و چاپگر :

این سیستم عامل برای سرویس اشتراک فایل و چاپگر خود بسیار معروف است.این سرویس فایل ها را برای دسترسی کاربران شبکه به اشتراک قرار می دهد ومی تواند چاپگر را برای استفاده مشترک کاربران شبکه در

دسترس قرار دهد. این سیستم عامل اولین سیستم و شاید بتوان گفت که بهترین آنها برای اجرای این سرویس می باشد.

پشتیبانی از نرم افزارهای کاربردی :

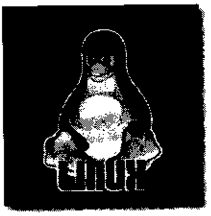
یکی از نقاط ضعف این سیستم عامل در این بخش است.این سیستم عامل تنها برای سرور تهیه شده از این رو تنها سرویس های شبکه به خوبی اجرا می گردد و امکان اجرای نرم افزار های جانبی را ندارند که این امر را می توان مهمترین نقطه ضعف آن دانست.

امنیت :

این سیستم عامل را می توان یکی از امن ترین سیستم عامل ها دانست. در این سیستم عامل کلمه کاربری و رمز عبور کد گزاری می شوند به علاوه که قبل از ورود به سیستم شما هیچ کدام از منابع شبکه را نمی توانید مشاهده نمایید و استفاده از منابع سیستم تنها برای کاربرانی که به سیستم وارد شده اند مجاز است. برای این منظور نام کاربری و کلمه عبور به بانک اطلاعاتی مرکزی سیستم ارسال می گردد و در آنجا بررسی می گردد که آیا اطلاعات وارد شده صحیح است در اینصورت اجازه ورود به سیستم به کاربر داده می شود.

این سیستم توسط آژانس امنیت ملی آمریکا (NCA) به عنوان سیستم عاملی امن معرفی شده که در دستگاه های دولتی و امنیتی می تواند مورد استفاده قرار گیرد.

Unix / Linux :



نسخه های مختلفی از سیستم عامل لینوکس امروزه در دسترس هستند. هسته اولیه این سیستم عامل یونیکس بود که در سال۱۹۶۹ بنا نهاده شد که لینوکس بخشی از آن هسته اولیه بود. لینوکس اولیه فاقد رابط گرافیکی بود که تمامی فرامین از خط فرمان اجرا می شد اما امروزه دارای رابط های گرافیکی زیادی شده است که کار با آن را آسانتر نموده و محبوبیتش را افزایش داده است.

امکانات :

سیتم عامل یونیکس از هسته اصلی با نام kernel تشکیل شده است است تشکیل شده است. این هسته وظیفه دسترسی به سخت افزار و برقراری ارتباط با رابط های کاربری را برعهده دارد. رابط های کاربری می تواند خط فرمان یا رابط های گرافیکی باشند که به کاربر کمک می نمایند تا با سیستم عامل ارتباط برقرار نماید.

لینوکس سیستم عاملی بود که با توسعه کرنل سیستم عامل یونیکس توسط لینوس تروالدز در سال ۱۹۹۴ در دانشگاه هلسینکی فنلاند تهیه شد. این سیستم عامل عمدتا رایگان بوده و منابع آن نیز بصورت رایگان در اختیار توسعه دهندگان نرم افزار قرار گرفته است که این امر کمک شایانی برای رشد و توسعه سریع آن نمود.

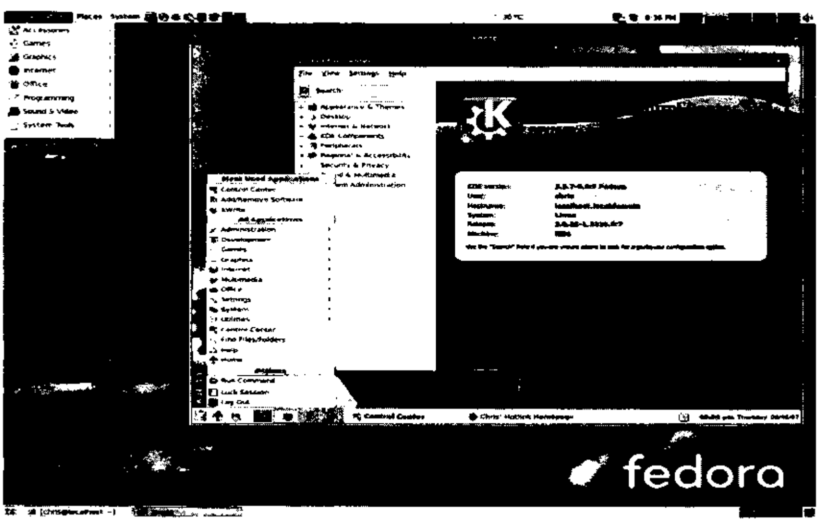
توسعه دهندگان به سرعت توانستند آن را برای استفاده های خاص و پشتیبانی از زبان های محلی و سیستم های سخت افزاری خاص پیکربندی نمایند. نسخه هایی از این سیستم عامل برای استفاده در سیستم های اپل شرکت مکینتاش توسعه یافتند که امروزه در این سیستم ها استفاده می شوند.

نسخه های مختلفی امروزه در دنیای شبکه مورد استفاده قرار می گیرند که با توجه به امکاناتشان معمولا برای مقاصد خاصی مورد استفاده قرار می گیرند. برخی از آنها عبارتند از :

- RedHat Linux
- Debian
- UBUNTU
- Slackware
- Openlinux

رابط کاربری :

رابط گرافیکی زیر با نام KDE است که بر روی یکی ازنسخه های لینوکس با نام fedora که از خانواده RedHat می باشد؛ نصب شده است.



پشتیبانی از کاربران وسازگاری با سیستم های دیگر:

سرور های یونیکس همگی از پروتکل های استاندارد اینترنت پشتیبانی می نمایندبرخی از این پروتکل ها عبارتند از : HTTP,TCP/IP,FTP,LPR

استفاده از این ایده باعث شد که تمامی سیتم عامل های شبکه از پروتکل TCP/IP و دیگر پروتکل های استاندارد اینترنت برای ارتباطات و سرویس های شبکه خود استفاده نمایند. این کار باعث ایجاد یک هماهنگی در بین سیستم عامل های مختلف شبکه می شود.

سنجش اعتبار:

در این سیستم عامل روش های متفاوتی برای سنجش اعتبار کاربران استفاده می شود. البته این امر بستگی مستقیم به این دارد که سیستم عامل یونیکس یا لینوکس باشد و چه نرم افزاری برای این کار مورد استفاده قرار گیرد .

برخی از پروتکل کربروس استفاده می نمایند و برخی هم موارد امنیتی را از سرور مدیریت کاربران شبکه مانند NDS یا AD دریافت می نماید.

اشتراک قراردادن فایل و چاپگر :

شاید این نکته را بدانید که سرویس اشتراک فایل و چاپگر در این سیستم عامل بر بستر TCP/IPعمل می نماید پروتکل های شبکه مانند HTTPو FTPدر این سیستم براحتی عمل می نمایند. برای اشتراک چاپگر از LPD/LPR بهره می گیرد. نرم افزاری در سیستم عامل یونیکس با نام سمبا (Samba) وجود دارد که یونیکس را همانند یک سرور ویندوزی نمایش می دهد وبرای انتقال فرامین از پروتکل SMB (Server Message Block) یعنی همان پروتکلی که ویندوز از آن استفاده می کند بهره می برد.

پشتیبانی از نرم افزار های جانبی :

همانگونه که در این بخش گفتیم یونیکس قدیمی ترین سیستم عامل شبکه می باشد. از این رو تعداد نرم افزار های جانبی برای این سیستم عامل بسیار زیاد است. اما خبر بد این است که هر نرم افزاری برای اجرا در یک نسخه خاص طراحی شده است و این تعداد نرم افزار ها در هر یک از نسخه ها بسیار محدود می نماید. همچنین اکثر نرم افزار ها بصورت رایگان تهیه شده اند که عمدتا فاقد پشتیبانی مناسب در هنگام بروز اشکال هستند.

امنیت :

تنها بخش کوچکی از نسخه های لینوکس به روز و کارآمد در دنیای شبکه باقی می ماند و بخش عمده آنها به مرور زمان دیگر به روز رسانی نمی شوند. این امر خطرات امنیتی را در شبکه را افزایش می دهد . اما نکته مهمی که باعث دلگرمی مدیران شبکه می شود این است که منابع این سیستم عامل ها باز بوده و مدیران خود می توانند با توسعه این نرم افزار ها مشکلات امنیتی موجود را با توجه به ساختار و نیازهای شبکه خود شناسایی و برطرف نمایند.

: Macintosh

شاید شما هم با ما هم عقیده خواهید بود که رابط کاربری این سیستم عامل را بتوان راحت ترین رابط برای کاربران دانست.این رابط در سال ۱۹۸۳ توسط شرکت Apple برای سیستم عامل Macintosh که آن را به اختصار Mac OS میگویند ؛طراحی گردید.

ترکیب سیستم عامل و رایانه های این شرکت به دلیل سهولت کاربرد بسیار کاربر پسند هستند از این رو بسیاری از افراد برای اولین بار ترجیح می دهند که از این سیستم ها استفاده نمایند.

صرفنظر از برخی استثنا ها ؛ سیستم عامل Mac OS تنها بر روی سیستم های سخت افزاری Macintosh قابل نصب و استفاده است.

در این بخش شما با برخی خصوصیات این سیستم عامل بیشتر آشنا می شوید. این خصوصیات عبارتند از:

امکانات :

این سیستم در طول عمر خود نسخه های زیادی به بازار عرضه کرده است که در هر نسخه جدید امکانات بسیاری به آن افزوده شده است.برای آشنایی با این سیستم عامل لازم است که مقداری در مورد گذشته و سیر تحول آن بیشتر بدانیم.

سیستم ۱ :

نسخه اصلی این سیستم عامل در سال ۱۹۸۴ معرفی گردید.رابط گرافیکی این سیستم عامل در آن دوره بسیار ساده و فاقد رنگ بود و کلا از رنگ پشتیبانی نمی کرد اما رابط کاربری آن بسیار قوی بود که در آن دوران طرفداران زیادی داشت.

سیستم ۶ :

این نسخه در سال ۱۹۸۶ معرفی شد. بسته به امکانات گرافیکی سخت افزاری توان نمایش هزاران و شاید میلیون ها رنگ را داشت که در آن دوران برای کاربران بسیار جالب و هیجان انگیز بود.

سیستم ۷ :

این نسخه تمامی امکانات نسخه ۶ را داشت اما نسخه های قبلی امکان پردازش همزمان تنها یک درخواست را داشتند. در نسخه ۷ امکانی برای اجرای همزمان چندین نرم افزار به سیستم عامل افزوده شد. برخی امکانات مانند استفاده از فضای دیسک به عنوان حافظه مجازی و اشتراک فضا بر روی شبکه هم در این نسخه افزوده شد.

Mac OS 8 :

در سال ۱۹۹۷ تغییرات زیادی در سیستم عامل بوجود آمد.اولین تغییر در نام سیستم بود. سیستم عامل به Mac OS تغییر نام داد. تغییر بعدی استفاده از مرورگر اینترنت مایکروسافت به عنوان مرورگر پیش فرض سیستم بود که در راستای تعامل با مایکروسافت انجام شد.یک ماشین اجرای نرم افزار های جاوا هم به سیستم عامل افزوده شد و همچنین نحوه تبادل داده ها با سیستم عامل های دیگر هم ارتقا پیدا کرد.

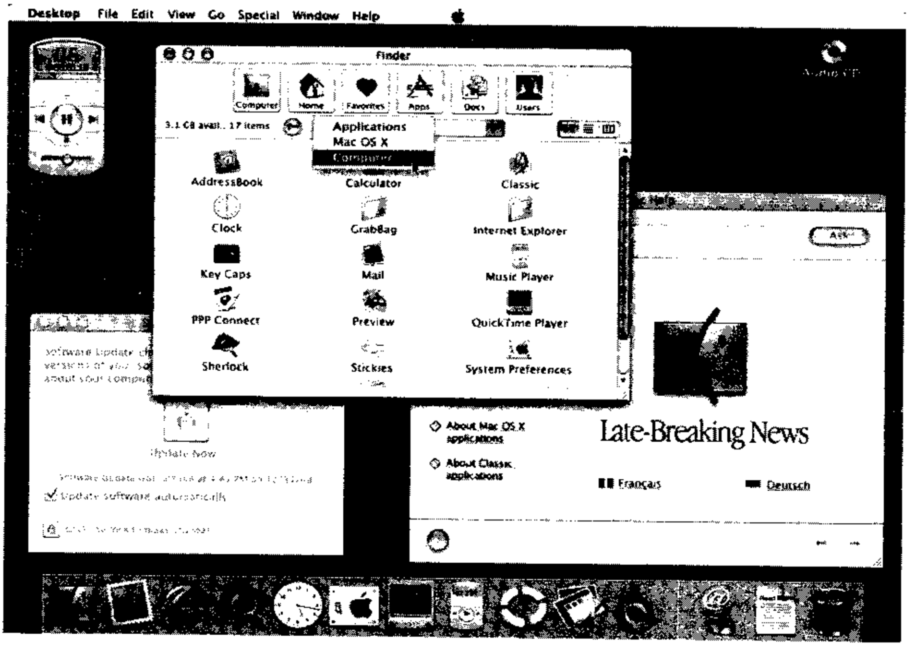
Mac OS 9 :

در این نسخه بیشتر سعی بر ارتقای سرویس ها و امکانات بود.سیستم پردازش همزمان درخواست ها ارتقا یافت و مرورگر برای شبکه هم به سیستم عامل افزوده شد که کاربران بتوانند کاربران و سرور های شبکه را براحتی جستجو نمایند. سرویس ذخیره سازی کلمه عبور هم بسیار تقویت شد.

Mac OS X (OS10) :

در میان آشفته بازار سیستم های عامل ؛شرکت Apple بالاخره سیستم عامل خود با نام OS X در سال ۲۰۰۱ معرفی نمود. در این نسخه با کمک گرافیک و رنگ توانست محیط کاربری بسیار قوی و کارآمد طراحی نماید. این نسخه بر روی هسته یونیکس طراحی شده بود که آن را بسیار قوی و قابل اعتماد می ساخت . همچنین در این نسخه امکان ذخیره در فرمت PDF به اکثر نرم افزار ها اضافه شد.

رابط کاربری :



پشتیبانی از کاربران :

پشتیبانی از کاربران در سرور های Mac OS دارای محدودیت هایی است. همانگونه که واضح است سرور های Mac OS از کاربران Macintosh پشتیبانی می نمایند اما سرویس Samba در نسخه های امروزی این سیستم عامل امکان سنجش ورود کاربران و اتصال آنها به شبکه را امکانپذیر ساخته است.

سرور های Mac OS شاید یکی از بهترین گزینه ها برای سرور اشتراک فایل باشد زیرا هسته اصلی این سیستم عامل یونیکس بوده و به دلیل هماهنگی یونیکس با پروتکل TCP/IP بهترین کارایی را برای این امر دارند.

قابلیت ارتباط با سیستم های دیگر :

این سیستم به عنوان یک سرور بسیار قوی و قابل اعتماد است اما براستی نمی توان آن را با سیستم عامل یونیکس در سیستم های بسیار بزرگ مقایسه نمود و باید تنها به استفاده در شبکه های کوچک بسنده کرد.

این سیستم عامل با گروه وسیعی از کاربران سازگار است. اما نکته مهم این است که اکثر کاربران در بخش های تجاری از سیستم عامل ویندوز استفاده می نمایند دلیل آن هم این نکته است که اکثر نرم افزارهای کاربردی این بخش برای سیستم عامل ویندوز طراحی شده و نمونه این نرم افزار ها برای سیستم عامل های دیگر بسیار اندک و عمده آنها نا کارآمد هستند.

سیستم عامل ویندوز در نسخه های سرور خود امکان پشتیبانی از کاربران این سیستم عامل را پیش بینی نموده و قرار داده است. این پشتیبانی بسیار دقیق و کامل است بطوریکه کاربران متوجه اختلاف بین سرور های ویندوز و Mac OS نمی شوند.

تصدیق ورود :

سنجش اعتبار کاربر در این سیستم عامل با کمک مکانیزم کربروس (Kerberos) انجام می گیرد. علاوه بر آن این سیستم دارای امکانی است با نام Keychain که تمامی کلمه عبور هایی که مورد استفاده شما قرار می گیرد(مانند کلمه عبور سرویس FTP و کلمه عبور در وب سایت ها) را در محل خاصی ذخیره می کند. هرگاه کاربر بخواهد از فضایی استفاده نماید که کلمه عبور آن قبلا ذخیره شده است؛ این سرویس کلمه عبور را به جای کاربر وارد نموده و امکان ورود به آن فضا را براحتی برای کاربر فراهم می نماید.

علاوه بر این امکانات ؛ نسخه های جدید این سیستم عامل از سیستم مدیریت کاربران سیستم عامل Apple با نام Apple 's Open Directory پشتیبانی می نمایند.این سیستم عملکردی شبیه سیستم مدیریت کاربران در ویندوز و ناول دارد و امکان سنجش اعتبار کاربران از طریق یک بانک اطلاعاتی مرکزی را فراهم می آورد.

اشتراک قراردادن فایل و چاپگر :

این سیستم عامل می تواند عملکرد های بسیاری در شبکه داشته باشد.علاوه بر استفاده به عنوان یک کاربر شبکه، می تواند یک سرور برای اشتراک قراردادن فایل و چاپگر با استفاده از پروتکل AppleShare باشد.

یکی از مزایای استفاده از این سیستم عامل مدیریت بسیار آسان آن است. در بسیاری از شرکت های کوچک که بودجه کافی برای استخدام کارشناس شبکه ندارند استفاده از این سیستم عامل برای اشتراک قراردادن در این شرایط بهترین گزینه خواهد بود.

پشتیبانی از نرم افزارهای کاربردی :

این سیستم عامل تنها نرم افزارهای نسخه های قدیمی خود و برخی از نرم افزارهای یونیکس که برای استفاده در این سیستم عامل تغییر یافته اند را پشتیبانی می کند. باتوجه به توانایی ها و امکانات این سیستم عامل برخی توسعه دهندگان نرم افزار بسته های نرم افزاری برای این سیستم تهیه کرده اند. البته در اکثر اوقات از این سیستم عامل می توان به عنوان سرور در شبکه های کوچک و متوسط استفاده می شود از این رو در نسخه های سرور با برخی سرویس ها مانند Apache یک سرویس دهنده میزبانی شبکه وب و MySQL که یک بانک اطلاعاتی بسیار قوی است ارایه می گردد.

امنیت :

این سیستم عامل امنیت قابل اعتماد را فراهم می آورد.این سیستم امنیت کاربران را به عنوان بخشی از سیستم عامل تعریف نموده و برخی سرویس ها که امکان نفوذ از طریق آنها به سیستم وجود دارد توسط سیستم عامل غیر فعال شده است. این مسائل این سیستم عامل را امن ترین سیستم عامل شبکه تبدیل نموده است.

جمع بندی:

در این بخش شما:

- ❖ درخصوص امکانات و خصوصیات سیستم عامل یونیکس و لینوکس مطالب مهمی آموختید.
- ❖ درخصوص امکانات و خصوصیات سیستم عامل ناول مطالب مهمی آموختید.
- ❖ درخصوص امکانات و خصوصیات سیستم عامل ویندوز مطالب مهمی آموختید.
- ❖ درخصوص امکانات و خصوصیات سیستم عامل مکینتاش مطالب مهمی آموختید.

سوالات ارزیابی برای آزمون +Network :

۱ -کدامیک از این سیستم های عامل دارای رابط گرافیکی هستند. (تمامی موارد صحیح را مشخص نمایید)

الف) ویندوز ۲۰۰۳
ب) لینوکس
ج) مکینتاش
د) ناول نت ویر

۲-کدام سیستم عامل از دیگر سیستم عامل ها امن تر است.

الف) ویندوز
ب) یونیکس
ج) ناول
د) مکینتاش

۳-کدام گزینه از نسخه های لینوکس است . (تمامی موارد صحیح را مشخص نمایید)

الف) Os X
ب) fedora
ج) Ubuntu
د) RedHat

۴- کدام سیستم عامل را می توان معمولترین و متداولترین و محبوبترین سیستم در بین کاربران دانست.

الف) ویندوز
ب) یونیکس
ج) لینوکس
د) مکینتاش

۵-کدام سیستم عامل نیاز به سخت افزار خاص برای نصب و استفاده دارد.

الف) ویندوز ۲۰۰۳
ب) لینوکس
ج) یونیکس
د) مکینتاش

۶- سرویس Apache بر روی کدام سیستم عامل نصب می شود.
الف) ویندوز ۲۰۰۳
ب) لینوکس
ج) ویندوز ۲۰۰۰
د) ویندوز NT

۷- سیستم مدیریت کاربران ویندوز کدام گزینه است . (تمامی موارد صحیح را مشخص نمایید)
الف)اکتیو دایرکتوری
ب) NDS
ج) Edirectory
د) بایندری

۸-کدامیک از این سیستم های عامل بر مبنای یونیکس اجرا شده اند . (تمامی موارد صحیح را مشخص نمایید)
الف) ویندوز
ب) ناول
ج) مکینتاش
د) لینوکس

۹- نرم افزاری که مدیریت منابع شبکه را بر عهده دارد ....می باشد.
الف) نرم افزار مدیریت کاربران.
ب) سیستم عامل.
ج) نرم افزار شبکه .
د) نرم افزار کاربردی مدیریت شبکه.

۱۰-بیشترین پشتیبان از نرم افزار های جانبی همچنین بیشترین نرم افزار های کاربردی مربوط به کدام سیستم عامل است.
الف) ویندوز
ب) لینوکس
ج) ناول
د) یونیکس

پاسخ به سوالات این بخش

۱ - **الف ، ب ،ج ،د**

ناول تنها در نسخه های جدید رابط گرافیکی افزودنی دارد.لینوکس و مکینتاش هم رابط گرافیکی به آن اضافه می شود. تنها سیستم عامل ویندوز است که رابط گرافیکی جزیی از سیستم عامل است.

۲ - **ب**

چون تنها یک گزینه صحیح است و مقایسه باید انجام شود امن ترین سیستم عامل یو نیکس است

۳ - **ب ،ج ،د**

با توجه به توضیحات این فصل مشخص است که پاسخ اشتباه الف است زیرا Os x نسخه ای از سیستم عامل مکینتاش است.

۴ - **الف**

از دید کاربران معمولترین و متداولترین سیستم عامل است.

۵ - **د**

بجز موارد استثنایی این سیستم عامل تنها بر روی سخت افزار خود نصب می گردد.

۶ - **ب**

این سرویس یکی از سرویس های سیستم عامل لینوکس است.

۷ - **الف**

اکتیو دایرکتوری یا AD مدیریت کاربران در سیستم عامل ویندوز را بر عهده دارد.

۸ - **ج**

مکینتاش و لینوکس بر روی هسته اصلی یونیکس ارتقا یافته اند.

۹ - **ب**

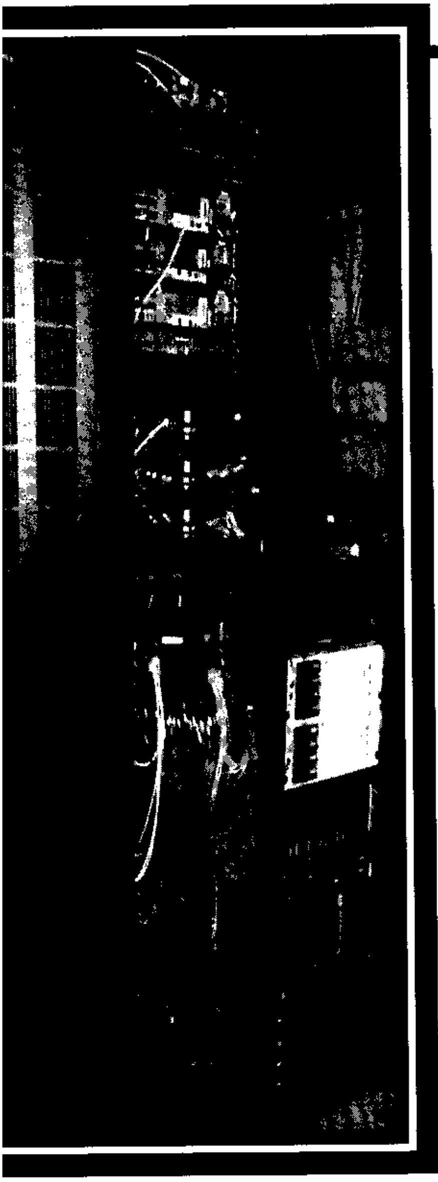
مطابق با تعاریف این فصل سیستم عامل مدیریت منابع شبکه را به عهده دارد. نرم افزار های کاربردی تنها به سیستم عامل در این راه کمک می نمایند.

۱۰ - **الف**

به دلیل اینکه محبوبترین سیستم عامل در بین کاربران است بیشترین نرم افزار های کاربردی مربوط است به سیستم عامل ویندوز.

فصل ششم

شبکه های سیمی و بیسیم



شما در این فصل با این مفاهیم آشنا خواهید شد:

۶-۱ شناسایی خصوصیات کلی مانند : سرعت انتقال ؛فرکانس ؛ نحوه انتقال و توپولوژی در شبکه های بدون سیم زیر :

- 802.11
- مادون قرمز
- بلوتوث

۶-۲ آشنایی با عوامل مهم که بر روی سرعت و محدوده پوشش شبکه های بدون سیم مانند :

- نوع آنتن
- عوامل جوی
- رابط اتصال

۶- ۳ شناسایی تجهیزات راه اندازی و عیب یابی شبکه های سیمی و همچنین موارد استفاده از هرکدام مانند:

- آزمایشگر کابل
- پانچ کننده کابل

مقدمه:

این بخش شما را به اولین و شاید مهمترین بخش عملی راهنمایی می نماید :توانایی راه اندازی سخت افزاری و نرم افزاری یک شبکه.

در این بخش سعی ما بر این است که مطالبی که شما برای راه اندازی یک شبکه جدید و یاپیش نیاز هایی که برای ارتقا یک شبکه قدیمی نیاز دارید و مواردی که برای اجرای یک شبکه می بایست راه اندازی و پیکر بندی گردد را در اختیار شما قرار دهیم. این موارد شامل شبکه های سیمی و بدون سیم خواهد بود .

مواردی که پیش از راه اندازی باید بدانید:

پیش از افزودن یک سخت افزار ؛ارتقا سیستم عامل ؛نصب یک نرم افزار جدید و یا ایجاد هر تغییر جدید در شبکه می بایست یک تصویر کامل از شرایط حال حاضر شبکه در اختیار داشته باشید. همچنین شما می بایست اطلاعات کافی درمورد نحوه عملکرد و وظایف هریک از اجزای شبکه در حالت عادی داشته باشید تا در صورت بروز شرایط اضطراری بتوانید شبکه را مدیریت نمایید.

همچنین یکی دیگر از وظایف هرکارشناس بررسی وقایع ثبت شده و پیام های خطای شبکه است. با این کار شما می توانید از سوابق خطاها و وضعیت سلامت شبکه آگاه شوید.

آخرین نکته مطالعه مستنداتی است که از سوی شرکت سازنده همراه سخت افزار و یا نرم افزار ارایه شده است. با ۱۵ دقیقه مطالعه این اسناد شما ممکن است از اتلاف ده ها ساعت وقت خود پیشگیری نمایید.

دستورالعملهای اجرایی استاندارد :

دستورالعملهای اجرایی استاندارد بخشی از سیاست های اجرایی شرکت ها هستند و معمولا همه چیز را پوشش می دهند، از شرایط عادی شبکه تا موارد اختلال در شبکه ها و یا نحوه عملکرد و وظایف هر سیستم کامپیوتری در این دستور العمل پیش بینی می شود. به ویژه ، برای مدیران شبکه لازم است تا از سیاست های شرکت در خصوص موارد زیر آگاه باشند :

- دسترسی به اینترنت
- استفاده از چاپگر
- تخصیص فضای ذخیره سازی
- استفاده از سرویس پست الکترونیکی
- مدیریت بر کاربران

سیاست های در مورد این مسائل در سیستم نامگذاری شبکه منعکس می شود. این امر پروتکل های استاندارد و تنظیمات شخصی کاربران و محل دستگاه های شبکه را تحت تأثیر قرار دهد.

سیستم نامگذاری:

در این سیستم مشخص می شود که هریک از اجزای شبکه بر اساس قواعد سیستم عامل چگونه نامگذاری شوند.هر نام می بایست در شبکه منحصر بفرد باشد و در یکی از گروه های زیر طبقه بندی شود.

- سرور ها
- چاپگر ها
- نام کاربری کاربران
- گروه های کاربران
- گروه آزمایش و خدمات

نامگذاری سرور ها :

بطور کلی؛ نام سرور ها بر اساس عملکرد و یا محل قرار گرفتن آن تعیین می شود و در برخی موارد هم نام ها ترکیبی از ۲ حالت هستند.به عنوان مثال سروری که دربخش فروش قرار دارد ممکن است نامش "فروش "و یا با قرار گرفتن آن در شهر تهران نامش "فروش تهران " تعیین شود.

حالت دیگر استفاده از شماره برای سرور ها می باشد.می توان سرور ها با کاربرد یکسان را با شماره مشخص نمود. روش معمول امروزی استفاده ترکیبی از نام و محل قرار گرفتن سرور می باشد.در این روش ممکن است در نام سرور شما ۳ حرف نمایانگر شهر و ۳ حرف نمایشگر عملکرد آن سرور باشد و عددی هم نمایشگر شماره آن سرور در بین دیگر سرور ها باشد.

نامگذاری چاپگر ها :

همانند نام سرور ها ؛ نام چاپگر ها هم می تواند براساس نام ؛ عملکرد و یا ترکیبی از هر دو مورد باشد. با این کار امکان یافتن این چاپگر برای کاربران شبکه آسانتر می شود. البته می توان در این نام نوع چاپگر را هم مشخص نمود که به کاربران برای انتخاب چاپگر مناسب کمک خواهد نمود.

> استفاده از این روش برای نامگذاری پیشنهادی است و هیچ اجباری برای استفاده از این روش نمی باشد. این روش را می توان یکی از روش های صحیح نامگذاری دانست .

نامگذاری نام کاربری:

در حالت کلی ؛ معمولترین نام کاربری برای هرکاربر نام او می باشد.این روش تنها برای شبکه هایی با کاربران محدود و دفاتر کوچک قابل استفاده خواهد بود زیرا ممکن است در شبکه دو کاربر با نام یکسان وجود داشته باشند که نامگذاری را دچار اشکال می نماید.

البته این روش دارای ایرادات امنیتی است زیرا نفوذگران می توانند به راحتی آن را حدس برنند و امنیت شبکه رادچار خطرات جدی نمایند.

نام کاربری در شبکه می بایست منحصر بفرد باشد تا از تداخل نام ها جلوگیری به عمل آید.در شبکه های متوسط و بزرگ نام شبکه را از ترکیب نام کاربر و بخشی که توسط مدیر شبکه به آن افزوده می شود و حتی الامکان آن را مختصر می نمایند تا منحصر بفرد بودن نام کاربری در شبکه حفظ شود.

نامگذاری گروه های کاربران:

گروه های شبکه؛ گروهی از اجزای شبکه هستند که بصورت مجازی با توجه به عملکردشان در یک دسته قرار می گیرند.این دسته بندی به مدیر شبکه برای مدیریت شبکه بسیار کمک می نماید.می توان قوانین دسترسی ها را به گروه نسبت داد، با این کار تمامی کاربران که عضو گروه شوند تابع قوانین آن گروه خواهند بود بدین ترتیب مدیریت شبکه بسیار آسانتر خواهد شد.

گروه آزمایش و خدمات:

زمانی که شما تصمیم می گیرید یک نرم افزار و یا یک چاپگر جدید را بروی سیستم نصب نمایید بهتر است به عنوان کاربر مدیر نباشید و برای آزمایش به عنوان کاربری با دسترسی محدود باشید. دلیل این کار این است که درصورت بروز خطا هنگام نصب بر روی سیستم ؛ شما امکان ترمیم سیستم و رفع مشکلات را با کمک کاربر مدیر برای خود محفوظ خواهید نمود. کاربرانی که در این گروه قرار دارند می توانند بصورت محدود به منابع سیستم دسترسی داشته باشند.

پروتکل های استاندارد:

همانگونه که در مباحث قبلی ذکر کردیم ؛ هر پروتکلی دارای خصوصیات خاصی است. برای انتخاب پروتکل مناسب برای شبکه خود ، شما می بایست با خصوصیات تمامی پروتکل ها آشنا باشد.

به عنوان مثال اگر شما در شبکه ای قصد استفاده از اینترنت را ندارید و می خواهید کاربران شبکه با استفاده از نام خود در شبکه به فعالیت بپردازند گزینه مناسب برای شما NetBEUI است.زیرا این پروتکل قابلیت مسیریابی نداردو نام کاربران هم در شبکه استفاده می شود.

البته امروزه کمتر شبکه ای را پیدا خواهید نمود که از پروتکل TCP/IP استفاده نکند.زیرا می توان این پروتکل را عمومی ترین پروتکل دانست که قابل مسیریابی است و در شبکه اینترنت هم پروتکل اصلی به حساب می آید.

صرفنظر از پروتکلی که قصد استفاده از آن را دارید پیش از راه اندازی یا بروز رسانی شبکه؛ شما می بایست اطلاعات تمامی اجزا شبکه را در اختیار داشته باشید.این کار را می توانید با کمک ابزار کاربردی که در فصل ۴ به آن پرداختیم انجام دهید.

پیکر بندی ایستگاه های کاری :

رعایت یک استاندارد برای تمامی ایستگاه های کاری می تواند از جهات زیر مورد نظر قرار گیرد:

- به راحتی شما می توانید مشکلات کاربران را دنبال نموده و برطرف نمایید.
- رفع مشکلات کاربران به دلیل استفاده از سیستم عامل و تنظیمات شبکه یکسان به راحتی امکانپذیر می شود.

این موارد به این معنی نیست که تمامی کاربران از نرم افزارهای کاربردی یکسان استفاده نمایند.به عنوان مثال کاربران واحد مهندسی از نرم افزار های طراحی مانندCAD استفاده می نمایند حال آنکه واحد مالی از نرم افزار های حسابداری استفاده خواهد نمود.

بنابراین تنظیمات مربوط به هربخش از کاربران به گروه کاربری آنها نسبت داده می شود. در این حالت کاربرانی که در یک واحد مشغول کار هستند از نرم افزار ها و سیستم عامل یکسانی استفاده خواهند نمود.

همچنین می بایست نیاز های سخت افزاری حداقل برای هر ایستگاه کاربری هم در این استاندارد مورد توجه قرار گیرد. معمولا نیاز حداقل معمولا چند درجه پایین تر از حالتی است که یک سیستم می تواند با کیفیت و سرعت قابل توجه فعالیت نماید.

.مواردی که در یک سیستم باید مورد توجه قرار گیرد :

- نوع و سرعت پردازشگر
- حداقل حافظه جانبی
- حداقل حافظه اصلی
- نوع و سرعت کارت شبکه
- حداقل اندازه نمایشگر

محل قرار گرفتن تجهیزات :

با توجه به سیاست های اجرایی شبکه می توان مشخص نمود که هریک از اجزای شبکه باید درکجا قرار گیرند. این ملاحظات می تواند از نظر امنیتی باشد و یا این که محلی باشد که به منابع دیگر شبکه دسترسی داشته باشد و یا بتوان آنها را از سرما یا گرمای محیط در امان نگاه داشت.

البته در این طراحی نحوه قرار گرفتن تجهیزات، شما بیش از همه باید نیاز های کاربران را مدنظر قرار دهید که همیشه رضایت کاربران ، مدیریت شما بر شبکه را آسانتر می سازد.

مستند سازی شبکه



شاید برای همه ما بارها پیش آمده است که برای رفع اشکالات یک شبکه به محلی مراجعه کرده باشیم و در جواب درخواست ما برای ارایه مستندات شبکه تنها به ما خیره شده باشند و یا در بهترین شرایط با تعدادی برگه ناقص و یا حتی فاقد ارزش مواجه شده باشیم. در آن زمان شما می بایست زمان زیادی را صرف نموده تا ابتدا با ساختار شبکه آشنا شده و سپس به دنبال رفع مشکلات شبکه باشید. پس از پایان این مراحل شما در می یابید که برای پی بردن به پاسخ سوالی که ۵ دقیقه زمان می برد ؛ زمانی بالغ بر ۵ ساعت صرف کرده اید.

یکی از موانع مستند سازی شاید ترس و یا با عرض شرمندگی کوته نظری مدیر شبکه باشد. بسیاری از افراد مستند سازی را در تضاد با حظور خود در شبکه می دانند.آشنایی و شناخت از شبکه را اهرم فشار و برگ برنده خود می دانند تا شغل خود را حفظ نمایند که این اقدام را می توان کاملا غیر تخصصی و تا حدی کودکانه دانست. شاید نیاز به ذکر نباشد اما این نکته را همگان می دانند که مدیریت بر شبکه امری پیچیده است اما هر کارشناس با صرف زمانی کم یا زیاد می تواند بر شبکه تسلط پیدا نماید.

مستند سازی شبکه یک علم نیست و نیاز به تخصص بالایی ندارد. شما براحتی می توانید نقشه شبکه را ترسیم نموده و محل قرار گیری هریک از اجزای شبکه را در آن مشخص نمایید.در مرحله بعدی مشخصات فیزیکی وتنظیمات شبکه هر کاربر را هم به این نقشه اضافه نمایید. بدین ترتیب شما می توانید اجزای شبکه را مستند سازی نمایید. هر بار که به دلیل مشکلات شبکه به این نوشته ها مراجعه کنید متوجه خواهید شد که چه موارد دیگری هم مورد نیاز است که آن موارد را هم باید به مستندات خود اضافه نمایید.

عوامل زیست محیطی :

شرایط زیست محیطی یکی از عوامل تاثیرگزار در راه اندازی و یا بروز رسانی شبکه ها می باشد. همانند انسانها ؛ رایانه ها هم نیاز به شرایط اقلیمی مناسب برای ادامه فعالیت خود دارند. اگر شرایط آب و هوایی نا ملایم باشد رایانه نمی تواند با حداکثر توان خود فعالیت نماید.

در این بخش سعی می کنیم برخی از این عوامل که بیشتر اتفاق می افتند را بررسی نماییم :

فصل ششم- شبکه های سیمی و بیسیم

- ❖ مشکلات انرژی الکتریکی
- ❖ مشکلات الکتریسیته ساکن
- ❖ تداخل امواج الکترومغناطیسی
- ❖ تداخل امواج رادیویی
- ❖ مشکلات اقلیمی

مشکلات انرژی الکتریکی :

جریان متناوب که به منزله غذا برای تمامی تجهیزات الکتریکی می باشد. این جریان بر اساس واحد " ولت " سنجیده می شود .معمولا این جریان بین ۱۱۰ تا ۲۲۰ ولت می باشد.

هر انحرافی از این جریان مشکلاتی را برای تجهیزات ایجاد می نماید.عوامل ایجاد مشکلات به ۳ دسته تقسیم می شوند :

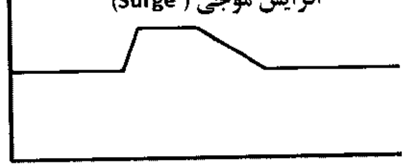
- ❖ افزایش جریان الکتریکی
- ❖ کاهش جریان الکتریکی
- ❖ کیفیت جریان

افزایش جریان الکتریکی :

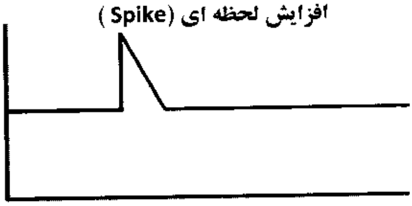
در این حالت انرژی زیادی وارد سیستم می گردد. این اختلال به دوصورت می تواند پدید آید :

- ❖ افزایش لحظه ای (Spike) : در این در حالت درطول یک ثانیه افزایش جریان الکتریکی و سپس بازگشت به حالت عادی انجام می گیرد.
- ❖ افزایش موجی (Surge) : در این در حالت جریان الکتریکی افزایش پیدا نموده و برای مدتی بیش از ۱ یا ۲ ثانیه در این حالت باقی می ماند و سپس به حالت عادی باز می گردد.

افزایش موجی (Surge)



افزایش لحظه ای (Spike)



معمولا افزایش موجی مدت زمان بیشتری طول می کشد به این دلیل خسارت آن از افزایش لحظه ای بیشتر است (البته ممکن است که این افزایش لحظه ای بسیار زیاد باشد که بتواند خسارت زیادی به بار آورد). در تصاویر گذشته شما تفاوت های این دو نوع افزایش جریان را مشاهده می نمایید.

برای جلوگیری از این افزایش ناگهانی تجهیزاتی مورد استفاده قرار می گیرند که عبارتند از :

- کنترل کننده افزایش موجی (Surge Protector)
- یکنواخت کننده جریان (Line Conditioner)

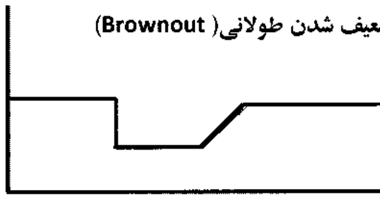
کنترل کننده افزایش موجی جریان در واقع یک مدار الکتریکی ویژه است که بر نحوه انتقال جریان نظارت می کند.هرگاه افزایش ناگهانی اتفاق افتادو جریان ورودی به حدی که در آن تنظیم شده است رسید ؛جریان ورودی را قطع می کند تا به تجهیزات آسیب نرسد. البته عیب این روش این است که حد تعیین شده بسیار بالاست که سیستم ها ممکن است قبل از رسیدن آن حد دچار آسیب شوند.البته بودن آن در شبکه از نبودنش بسیار بهتر است.

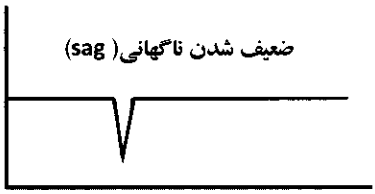
یکنواخت کننده جریان انتخاب بهتری نسبت به کنترل کننده افزایش جریان است. این دستگاه جریان ورودی را کنترل و آن را مطابق با استاندارد وارد سیستم می نماید.یکی از این تجهیزات UPS است. این دستگاه با کمک باتری و مبدل جریان الکتریکی ؛ جریانی ثابت و یکنواخت را برای تجهیزات متصل به خود فراهم می آورد. استفاده از این راه می تواند اکثر مشکلات جریان الکتریکی را برطرف نماید.

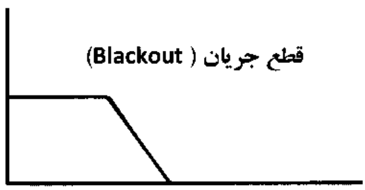
کاهش جریان الکتریکی :

- این اختلال زمانی بوجود می آیدکه میزان جریان الکتریکی کمتر از میزان استاندارد شود. معمولا ۳ نوع کاهش جریان مشاهده می شود:
- ضعیف شدن ناگهانی(sag) : این حالت برعکس حالت افزایش ناگهانی جریان می باشد.در زمانی کمتر از ۱ ثانیه جریان کمتر از سطح استاندارد می رود و مجدد به سطح استاندارد باز می گردد. در همین زمان اندک هم شما اثرات آن را مشاهده می نمایید. سوسو زدن چراغ ها و راه اندازی دوباره رایانه ها در این زمان اتفاق خواهد افتاد.
- ضعیف شدن طولانی(Brownout) : در این حالت افت جریان برای مدت طولانی تری ادامه خواهد داشت. در این مدت چراغ ها کم نور می شوند و پس از رفع مشکل به حالت طبیعی باز می گردند.
- قطع جریان (Blackout) : این حالت قطع کلی جریان می تواند برای مدت چند ثانیه؛دقیقه و یا شاید ساعت باشد.

در تصاویر زیر این اختلالات جریان را مشاهده می نمایید:







برای مقابله با این اختلالات گزینه مناسب شما UPS خواهد بود.این دستگاه حتی در زمان قطع کامل جریان هم می تواند انرژی مورد نیاز شما برای فعالیت را (برای مدت زمان محدودی بر اساس توان باتری های متصل به آن)فراهم آورد.

مشکلات کیفیت جریان :

این مشکلات زمانی بوجود می آید که فرکانس سرگردان در سیستم الکتریکی وارد منبع تغذیه سیستم شود.با ورود این جریان مزاحم سیستم دچار اختلالات عجیبی مانند راه اندازی مجدد سیستم و یا اختلال در عملکرد برخی تجهیزات می شود. برای شناسایی این موج مزاحم از دستگاه اسیلوسکوپ استفاده می شود. برای رفع این اختلال می بایست از یکنواخت کننده جریان و یا UPS استفاده نمود.

تخلیه الکتریسیته ساکن :

تخلیه الکتریکی زمانی اتفاق می افتد که دو جسم که دارای بار الکتریکی غیر همنام هستند به هم برخورد نمایند در این حالت الکتریسیته ساکن از سمت جسمی که بار الکتریکی بیشتری دارد به سمت جسم دیگر منتقل می شود این حالت معمولا به صورت جرقه قابل رویت است . این تخلیه الکتریکی می تواند باعث آسیب رساندن به قطعات حساس الکترونیکی تجهیزات شود به علاوه این تخلیه باعث ایجاد حسی ناخوشایند در کاربر هم می شود.

برای پیشگیری از این امر می بایست تمامی تجهیزات اتصال به زمین داشته باشند. اتصال به زمین باعث می شود که همیشه یک طرف خالی از الکتریسیته ساکن باشد و هیچگاه تخلیه الکتریکی انجام نگیرد.

تداخل امواج الکترومغناطیسی :

این تداخل زمانی بوجود می آید که یک میدان مغناطیسی کابل شبکه را احاطه کرده باشد. این امواج تقریبا در تمامی فضای دفاتر اداری حاظر هستند مثلا سیستم های تهویه مطبوع و بخاری های برقی منابع اصلی ایجاد میدان مغناطیسی هستند.

یکی از اشتباهات اساسی در هنگام راه اندازی یک شبکه ؛ قرار دادن کابل شبکه نزدیک لامپ مهتابی و یا کنار کابل های الکتریکی است زیرا این موارد مولد میدان مغناطیسی هستند. از این رو توصیه می شود یا از کابل هایی که دارای روکش مخصوص هستند(که انها را نسبت به اختلالات مغناطیسی و الکتریکی محافظت می نماید) استفاده شودو یا میان کابل های شبکه و کابل های الکتریکی فاصله ای منطقی رعایت شود.

راه پیشگیری از این تداخل استفاده از کابل هایی با روکش محافظ است. روکش محافظ آنها را نسبت به اختلالات مغناطیسی و الکتریکی محافظت می نماید.و روش دیگر استفاده از فیبر نوری است که کاملا نسبت به این نوع تداخل ها ایمن است

تداخل فرکانس رادیویی :

این تداخل زمانی پدید می آید که امواج رادیویی تحت تاثیر میدان الکتریکی حاصل از عملکرد تجهیزات الکترونیکی قرار گیرد. رادیو و تلویزیون را می توان عمده ترین استفاده کننده از این امواج به عنوان گیرنده و تلفن های همراه و بیسیم را عمده ترین استفاده کنندگان بصورت دو طرفه(گیرنده و فرستنده) دانست.



شناسایی این تداخل ها و پیدا کردن منبع این اختلال در بسیاری موارد بسیار مشکل وشاید غیر ممکن باشد. از این رو در صورت بروز اختلال می بایست با دقتی بسیار زیاد به دنبال منبع اختلال باشید. برای رسیدن به نتیجه در زمانی کمتر سعی نمایید که تمامی مواردی را که نسبت به آنها مشکوک هستید مرحله به مرحله از سیستم دور کنید تا بتوانید منبع اختلال را شناسایی نمایید

اختلالات آب و هوایی :

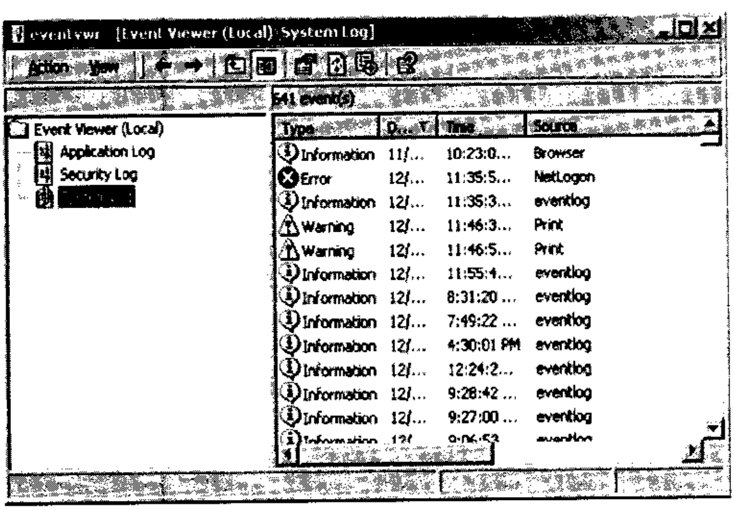
تجهیزات شبکه (مانند رایانه ها و سرور ها) نسبت به دمای هوا بسیار حساس هستند و ممکن است با افزایش دما دچار اختلال شوند.شرایط آب و هوایی که می بایست برای تجهیزات شبکه فراهم باشد تقریبا شبیه شرایط مورد نیاز بدن انسان است.دمای هوا بین ۲۰ تا ۳۰ درجه سانتیگراد و رطوبتی معادل ۴۰ تا ۶۰ درصد شرایط مناسب برای این تجهیزات می باشد.

برای جلوگیری از افرایش دما سیستم گردش هوا باید در اتاق سرور برقرار باشد. در اتاق سرور شما نباید از تجهیزات گرمایی استفاده نمایید همچنین تجهیزات خنک کننده شما نباید تولید رطوبت نمایند.

پیام های خطا و وقایع ثبت شده :

مطالعه دقیق پیام های خطا و وقایع ثبت شده اطلاعات کاملی نسبت به وضعیت سلامت شبکه در اختیار شما قرار می دهد.این اطلاعات از این بابت مورد اهمیت است که شما با دانستن وضعیت شبکه؛ هیچگاه تجهیزات جدیدی به شبکه ای که دارای مشکلات است اضافه نخواهید کرد.در وقایع ثبت شده تمامی اتفاقاتی که در سیستم رخ داده است ذخیره می شود. به عنوان مثال می توان زمان ورود و خروج کاربران به سیستم را مشخص نمود و یا زمان اضافه شدن یک رایانه به شبکه را مشخص نمود.

وقایع ثبت شده انواع مختلفی داردکه می توان به وقایع امنیتی ؛ وقایع سیستم ؛ وقایع نرم افزارهای کاربردی را اشاره نمود.در این تصویر نمونه وقایع ثبت شده سیستم را مشاهده می نمایید.



تنظیمات فعلی سیستم :

یکی از مسائل بسیار مهم در هنگام ارتقای شبکه و یا افزودن سخت افزار به آن دانستن تنظیمات سخت افزاری و نرم افزاری فعلی درسرور ها و سیستم کاربران شبکه است. این اطلاعات در زمانی تهیه می شود که شبکه بصورت عادی مشغول فعالیت است ونمایشگر فعالیت طبیعی آن است و پس از هر تغییری می بایست تنظیمات فعلی مجدد اعمال گردد.

مستندات دیگر :

گروه دیگری ازمستندات که در دسترس شماست و قبل و هنگام راه اندازی بسیار می تواند به شما کمک کند شامل موارد زیر هستند:

- فایل های راهنما
- اطلاعات فنی ارایه شده توسط شرکت سازنده تجهیزات یا ارایه کننده نرم افزار
- اطلاعات فنی ارایه شده در وب سایت رسمی شرکت سازنده تجهیزات یا ارایه کننده نرم افزار

البته برخی مدیران شبکه صحبت کردن با بخش پشتیبانی شرکت سازنده تجهیزات را بر مطالعه این منابع ترجیح می دهند.البته در بسیاری از موارد مکالمه با بخش پشتیبانی و دریافت راهنمایی رایگان نبوده و راهنمایی در قبال دریافت هزینه انجام می شود که شاید مقرون به صرفه نباشد.

شبکه های بی سیم

امروزه شبکه های بی سیم بسیار همه گیر شده است. شما می توانید نمونه ای شبکه ها را در بسیاری از مکان های عمومی مانند فرودگاه ؛ کتابخانه ، دانشگاه ها و هتل ها و همچنین در بسیاری شرکت های بزرگ مشاهده نمایید. از این رو دانستن مبانی و استاندارد های این شبکه برای تمامی کارشناسان فنی شبکه لازم است.

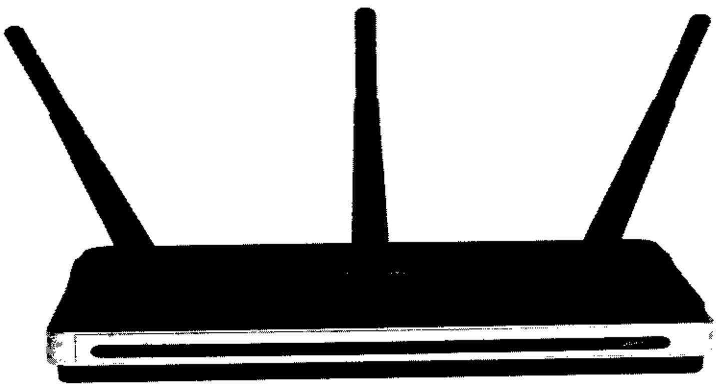
اجزای شبکه بی سیم:

شبکه های بی سیم در مقایسه با شبکه های سیمی از پیچیدگی های کمتر برخوردار است. زیرا رسانه انتقال هوا است و تنها فرستنده و گیرنده در این شبکه فعالیت دارند که رفع اشکالات این شبکه را بسیار آسان می نماید.

نقطه دسترسی بی سیم (Wireless Access Point) و کارت شبکه بی سیم (Wireless NIC) اجزایی هستند که در یک شبکه وایرلس وجود دارند.

نقطه دسترسی بی سیم (WAP):

در شبکه های سیمی در مرکز شبکه یک سوییچ قرار دارد که وظیفه اتصال سیستم ها به هم را بر عهده دارد. در شبکه های وایر لس هم شرایط یکسان است اما با رسانه ای دیگر درگیر هستند . دستگاهی که این دسترسی به شبکه را فراهم می می آورد، نقطه دسترسی بی سیم یا وپ نامیده می شود. نمونه ای از این دستگاه را در شکل زیر مشاهده می نمایید.

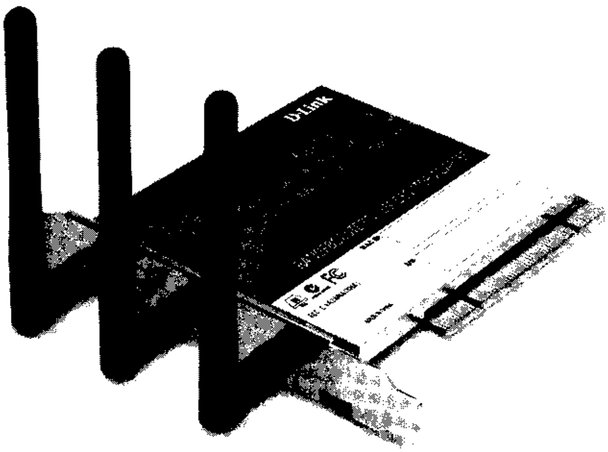


این دستگاه می تواند در حالت های مختلفی فعالیت نماید. برخی از آنها پل ارتباطی بین شبکه های بی سیم و سیمی هستند و برخی از آنها می توانند به عنوان مسیریاب همزمان هم به شبکه های سیمی و هم به شبکه های بدون سیم متصل باشند وشاید از آنها برای تکرار سیگنال برای مسافت طولانی تر استفاده شود .

برای افزایش محدوده تحت پوشش ؛ آنتنی بر روی این دستگاه نصب شده است . برخی دارای یک آنتن و برخی از مدل ها می توانند تا ۳ آنتن داشته باشند که هم محدوده پوشش را افزایش دهند و کیفیت شبکه بی سیم را ارتقا دهند البته در برخی سیستم ها این آنتن ها داخلی بوده و در ظاهر آنها فاقد آنتن هستند.

کارت شبکه بی سیم :

هر سیستمی که بخواهد به شبکه بی سیم متصل شود نیاز به یک کارت شبکه بی سیم دارد. وظیفه این دستگاه همانند همنوع خود در شبکه های سیمی است اما با این تفاوت که بجای اتصال کابل شبکه دارای یک آنتن است که برای ارسال و دریافت امواج از آن استفاده می نماید.این دستگاه هم دارای انواع مختلفی است که هرکدام برای استفاده در استاندارد خاصی طراحی شده اند. استاندارد های شبکه های بی سیم را در بخش بعدی خواهیم آموخت.





خصوصیات آنتن های بی سیم :

در شبکه های بی سیم از آنتن ها هم برای ارسال و هم دریافت امواج استفاده می شود.بصورت کلی دو نوع آنتن وجود دارد :

- آنتن های تک جهته یا Directional که به آنها نقطه – به – نقطه (Point – To-Point) هم می گویند.
- آنتن های تمام جهات یا Omni-Directional که به آنها نقطه – به – چند نقطه (Point – To-Multi Point) می گویند.

بر اساس یک قاعده کلی آنتن های تک جهته که به "یاگی" مشهور هستند فاصله طولانی تری به نسبت آنتن های همه جهته را پشتیبانی می نمایند. زیرا انرژی خود را تنها در یک جهت متمرکز می نمایند.از دیگر نمونه های این آنتن ها می توان به Dish اشاره نمود که باید حتما در جهت فرستنده تنظیم شود اما قدرت دریافت آنها بسیار بیشتر از انواع دیگر آنتن ها می باشد.

اکثر نقاط دسترسی بی سیم از آنتن های همه جهته استفاده می نمایند زیرا باید پوشش را برای تمام کاربران که در همه مناطق کنار آن هستند را فراهم نماید. البته دامنه استفاده از آنتن ها تنها به شبکه ها محدود نمی شود.نمونه ای از آنتن همه جهته را می توان در آنتن خودروها مشاهده نمود که جهت حرکت خودرو در دریافت امواج هیچ تاثیری ندارد. و آنتن های تک جهته را در آنتن های تلویزیون مشاهده نمود که باید حتما در جهت خاصی تنظیم شود تا کیفیت امواج دریافتی مناسب و قابل قبول باشد.

آنتن ها بر اساس قدرت ارسال و دریافتشان رتبه بندی می شوند. واحد این رتبه بندی dBi یا dBd می باشد. هرچه این عدد در مقیاس dBi بزرگتر باشد آنتن می تواند فاصله بیشتری را پوشش دهد. آنتن ها با

توجه به نوع طراحی و مواد سازنده آنها برای مصارف داخلی و خارجی تولید می شوند.آنتن های خارجی باید نسبت به عوامل جوی بسیار مقاوم تر باشند.

اگر آنتن در فرکانس کمتر از ۱ گیگا هرتز طراحی شود واحد اندازه گیری dBd بوده و اگر بالاتر باشد واحد اندازه گیری در مبنای dBi خواهد بود.اگر بخواهیم مقایسه ای انجام دهیم ۲ عدد یکسان در هرکدام از این مقیاس ها ؛dBd بسیار قوی تر از dBi خواهد بود. برای تبدیل این دو مقیاس به هم از رابطه زیر استفاده می نماییم :

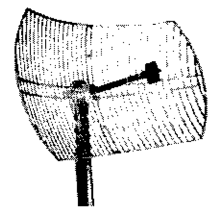
$$dBi = 2.2 + dBd$$

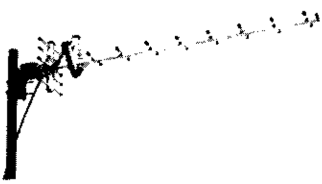
برای روشن شدن بحث به مثال های زیر دقت نمایید:

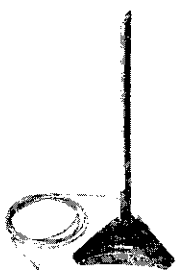
یک آنتن تک جهته با قدرت دریافت ۷ dBd معادل آنتنی با قدرت دریافت ۹/۲ dBi می باشد.

یک آنتن هم جهته با قدرت دریافت ۷ dBi معادل آنتنی با قدرت دریافت ۴/۸ dBd می باشد.

این محاسبات به شما کمک می نماید که بهترین انتخاب ممکن را برای آنتن انجام دهید اما شاید لازم به توضیح نباشد که در این مبحث ما تنها به معرفی و بیان برخی مقدمات می پردازیم.در صورت نیاز به مباحث پیشرفته لازم است که به موضوع آنتن ها در کتاب های شبکه بی سیم بصورت تخصصی مراجعه فرمایید.







آنتن های تک جهته یا Directional

آنتن تمام جهات یا Omni-Directional

راه اندازی شبکه های بی سیم

حال که با برخی مقدمات برای راه اندازی شبکه های بی سیم آشنا شدید وقت آن است که نحوه راه اندازی تجهیزات وشبکه بی سیم را فرا بگیریم.همانگونه که قبلا هم گفتیم این شبکه ها اجزای کمتر و در نتیجه پیچیدگی کمتری هم دارند.مواردی که باید برای اجرای این شبکه ها مورد توجه قرار گیرند به این شرح است :

فصل ششم- شبکه های بی سیم

- استاندارد های شبکه های بی سیم
- نحوه اتصال اجزای شبکه
- افت سیگنال (بررسی محل شبکه)

استاندارد های شبکه های بی سیم :

در مدتی که از عمر شبکه های بی سیم می گذرد،استاندارد های متعددی برای این شبکه ها تعریف شده است که همگی در زیر شاخه اصلی استاندارد IEEE 802.11 دسته بندی می شوند.البته برخی شبکه های بدون سیم هم با استفاده از بلوتوث و مادون قرمز تشکیل می شون که تابع این استاندارد نیستند . زیر شاخه های اصلی این استاندارد به شرح زیر است :

- 802.11 a
- 802.11 b
- 802.11 g
- 802.11 n

> علیرغم قرار داشتن این زیر شبکه ها در یک استاندارد ؛ اختلاف های فراوانی با هم دارند که می توان به سرعت و نحوه انتقال داده ها اشاره نمود که در مباحث بعدی به آنها خواهیم پرداخت.

شبکه مادون قرمز :

یکی از انواع شبکه های بدون سیم شبکه مادون قرمز است که امروزه مورد توجه قرار نمی گیرد.سیستم آن در کنترل از راه دور تلویزیون می باشد.این شبکه برای مسافت های بسیار کوتاه طراحی شده است و عمدتا برای اتصال سیستم های جانبی به رایانه استفاده می شوند.برخی از این تجهیزات مانند گوشی های تلفن همراه و صفحه کلید و موس رایانه وجود دارد.

حداکثر سرعت انتقال داده ها ۱۶ مگابیت در ثانیه بود که با ارتقای تکنولوژی به ۱۰۰ مگابیت در ثانیه در فاصله حد اکثر ۱ متر رسید. اگر از سرعت آن بگذریم فاصله ۱ متری نمی تواند پوشش مناسبی برای یک شبکه باشد. از این رو کمتر مورد توجه و استفاده قرار می گیرد.

شبکه بلوتوث :

یکی از استاندارد های جدید شبکه های بی سیم ، شبکه بلوتوث است. این شبکه برای جایگزین شدن با درگاه های مختلف ورودی در رایانه ها طراحی شد. اتصال هایی مانند صفحه کلید ؛موس و بلند گو می تواند حذف شده و این اتصال بی سیم جایگزین شود.

یکی از مزایای این تکنولوژی امکان اتصال همزمان چندین کاربر به بلوتوث است. امکانی که در مادون قرمز وجود ندارد.در مادون قرمز تنها دو دستگاه امکان اتصال به هم را دارند.

سرعت انتقال داده ها در این ارتباط ۱ مگابیت در ثانیه و حداکثر فاصله ۱۰ متر بود که با پیشرفت تکنولوژی سرعت انتقال و فاصله به ارتقا ۳ مگابیت در ثانیه یافت.البته در زمان نگارش این کتاب تلاش هایی برای تعریف استاندارد جدیدی با سرعت ۴۸۰ مگابیت در ثانیه در حال اجراست که به دلیل به نتیجه رسیدن آن فقط برای اطلاع شما ذکر می شود.

استاندارد 802.11 :

این استاندارد در زمان خود یک انقلاب تکنولوژیکی به شمار می رفت .سرعت انتقال در این شبکه ۲ مگابیت در ثانیه بود که در شرایط نا مناسب به ۱ مگابیت در ثانیه کاهش پیدا می کرد.این شبکه در محدوده فرکانس ۲/۴ گیگا هرتز فعالیت می نمود.این استاندارد در سال ۱۹۹۹ میلادی تغییر نمود و زیر شاخه هایی بر آن افزوده شد که در قسمت بعدی با آنها آشنا خواهیم شد.

استاندارد 802.11 a :

این زیر شاخه استاندارد 802.11 که سرعت انتقال داده ها را تا ۵۴ مگابیت در ثانیه افزایش می داد و محدوده فرکانس را ۵/۸ گیگا هرتز تغییر داد. این شبکه در فضای بسته معمولا ۷۵ متر و در فضای آزاد حدود ۳۵۰ متر را پوشش می دهد.

تکنیک های ارسال و دریافت در شبکه های بیسیم



دانستن این تکنیک ها فراتر از مبحث ما بوده و برای آشنایی بیشتر می بایست به کتابهای تخصصی شبکه های بی سیم مراجعه نمایید. اما در این بخش بصورت مختصر در این مورد مطالبی را ذکر می نماییم.

DSS: یکی از تکنیک های ارسال و دریافت در شبکه های بیسیم است. این تکنولوژی در استاندارد 802.11b استفاده می شود.این تکنولوژی نسبت به تداخل امواج مقاوم می باشد.یکی از محاسنش را می توان وجود سیستمی دانست که بخش های آسیب دیده داده ها را ترمیم می نماید.

FHSS: این تکنیک بسیار کم و به ندرت در شبکه هایی با استاندارد 802.11 مورد استفاده قرار می گیرد. در این روش داده ها برای انتقال در بین فرکانس های مختلف پرش انجام می دهند.یعنی برای ارسال یا دریافت داده ها در بخشی از هر ثانیه از یک فرکانس استفاده شده و بخش دیگر ثانیه فرکانس دیگری مورد استفاده قرار می گیرد. این زمان یعنی زمان پرش از هر فرکانس به فرکانس دیگر ۴۰۰ میلی ثانیه بصورت استاندارد تعریف شده است. بلوتوث از این تکنیک برای ارسال داده ها استفاده می نماید.

OFDM :استاندارد802.11a از این سیتم برای انتقال داده ها استفاده می نماید.در این سیستم داده ها در بین ۵۲ فرکانس حامل تقسیم شده و از این راه به مقصد می رسند. حسن این کار این است که گیرنده تنها همین بسته را که درحال دریافتش است می بیند. همچنین این تکنولوژی در مقابل تداخل فرکانس بسیار مقاوم می باشد و همچنین در مقابل افت سیگنال هم می تواند مقاومت بیشتری انجام دهد.

استاندارد 802.11 b :

هردو استاندارد 802.11 b و 802.11 a تقریبا در یک زمان معرفی شدند.با توجه به برخی مشخصات همانند ارزانتر بودن تجهیزات ؛محدوده پوشش به دلیل فرکانس پایین تر(هرچه فرکانس پایین تر باشد محدوده پوشش بیشتر خواهد بود) و هرچه فرکانس پایین تر باشد امکان تداخل فرکانس کمتر می شود همگی باعث می شود که استاندارد 802.11 b مورد توجه بیشتری قرار گیرد.

این شبکه در محدوده فرکانس ۲/۴ گیگا هرتز فعالیت می نماید و سرعت انتقال داده ها برابر ۱۱ مگابیت در ثانیه می باشد.و این شبکه در فضای بسته معمولا ۹۱ متر و در فضای آزاد حدود ۴۵۷ متر را پوشش می دهد .

اگرچه هردو استاندارد 802.11 b و 802.11 a از یک استاندارد مشتق شدند اما با هم سازگار نیستند.

Wi-Fiچیست ؟

شاید شما این علامت را در بسیاری از تجهیزات در استاندارد 802.11 b دیده باشید. این علامت تایید می نماید که این دستگاه برای ارتباط با تمامی تجهیزات که دارای این استاندارد هستند پیکربندی شده است.

استاندارد 802.11 g :

این استاندارد را می توان جامع ترین استاندارد در زمان خود بدانیم .زیرا هم سرعت انتقال داده های ۵۴ مگابیت در ثانیه را داشت و هم در فرکانس ۲/۴ گیگا هرتز فعالیت می نمود و از همه مهمتر این که با استاندارد b 802.11 هم سازگار بود.البته با ارتقای این استاندارد سرعت انتقال در +802.11 g به ۱۰۸ مگابیت در ثانیه افزایش یافت.

استاندارد 802.11 n :

این استاندارد مراحل نهایی ثبت خود را می گذراند. در این شبکه ها سرعت انتقال داده ها ۳۰۰ مگابیت در ثانیه می باشد و کاملا سازگار با استاندارد های b و g می باشد.زیر شاخه های این استاندارد با سرعت سرعت انتقال ۱۵۰ مگابیت در ثانیه هم امروزه معرفی شده است. البته پیش بینی ها از ارتقای سرعت این استاندارد در آینده تاسرعت ۴۵۰ مگابیت در ثانیه حکایت دارد.

حالت های نصب شبکه های بیسیم

فرض کنی که شما یک کارت شبکه و یک نقطه دسترسی بی سیم دارید و می خواهید که یک شبکه بی سیم راه اندازی نمایید.برای راه اندازی شبکه دو حالت کلی وجود دارد؛ حالت Ad-Hoc و حالت زیر ساخت که در این بخش به معرفی هر دوحالت می پردازیم.

حالت Ad-Hoc :

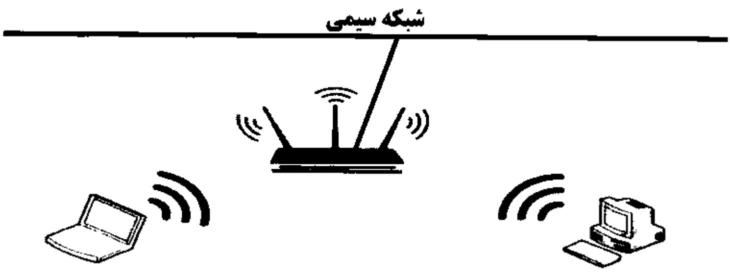
این حالت؛ ساده ترین حالت برای راه اندازی شبکه وایرلس است. ساده ترین حالت این است که دو سیستم می توانند بدون نیاز به هیچ دستگاه دیگری با هم تبادل داده انجام می دهند. نمونه ای از این حالت را در تصویر زیر مشاهده می نمایید.



حالت زیر ساخت :

یکی از راهکارهای استفاده از شبکه های بی سیم ؛ اجرای شبکه و امکان دسترسی کاربران این شبکه ها به منابع در شبکه های سیمی است.برای این کار تمامی اجزای شبکه وایرلس می بایست در حالت زیر ساخت پیکربندی شده باشند.

در این حالت تمامی اجزا تنها باید با نقطه دسترسی بی سیم (بجای ارتباط هریک از اجزا با هم در حالت Ad-Hoc) ارتباط داشته باشند. نقطه دسترسی از یک طرف با شبکه بی سیم و از سوی دیگر با شبکه سیمی در ارتباط است و از دید کاربران شبکه سیمی ؛کاربران شبکه بی سیم هم همانند آنها هستند.



برای اجرای یک شبکه در حالت زیر ساخت شما می بایست با برخی تعاریف آشنا شوید. SSID (شناسه امنیتی شبکه)و امنیت شبکه .

شناسه امنیتی شبکه یک شناسه منحصر بفرد است که متشکل از ۳۲ کاراکتر بوده و نمایانگر یک نام و مشخصه یک شبکه خاص می باشد.تمامی سیستم ها برای اینکه عضو یک شبکه یکسان شوند می بایست این نام را انتخاب نمایند.

قرار گرفتن تعدادی نقطه دسترسی در یک فضا که همگی دارای یک شناسه امنیتی یکسان باشند به کاربران این اجازه را می دهد که بتوانند در محدوده آن فضا بدون قطع شدن اتصال ، آزادانه حرکت نمایند. این حالت را Roaming یا حالت جابجایی می نامند.

امنیت شبکه های بیسیم :

همانگونه که می دانید امواج شبکه های بیسیم در محیط پراکنده می شوند و چه بسا از محدوده ساختمان خارج شوند همچنین نقاط دسترسی بصورت پیش فرض شناسه امنیتی خود را به نمایش قرار می دهند و کاربران می توانند آن را انتخاب نموده و به آن متصل شوند اینجاست که بحث امنیت شبکه مطرح می شود. جهت امن نمودن این شبکه ها ، نقاط دسترسی موارد امنیتی زیر را بر روی شبکه اجرا می نمایند:

(Wired-Equivalent Privacy protocol) : WEP

این روش بر اساس یک کد امنیتی که بر روی نقطه دسترسی تعریف می شود و تمامی کاربران که قصد ورود به شبکه را دارند می بایست آن کد را وارد نموده و به شبکه دسترسی پیدا نمایند. این کد ترکیبی از عدد و رقم می تواند باشد که توسط مدیر شبکه تعریف می گردد. این کد می تواند ۳۲ بیت تا ۲۵۶ بیت باشد که یا در مبنای ۱۰ و یا در مبنای ۱۶ تعریف می گردد.

(Wi-Fi Protected Access) : WPA

این روش هم برای رمز گذاری داده ها می باشد این روش جایگزین روش قبلی که دارای ضعف های زیادی بود؛ شده است.در این روش تمامی داده ها رمز گذاری و سپس منتقل می شوند که تا حد زیادی خلاء امنیتی شبکه های بیسیم را پر می نماید. نسخه های ارتقا یافته این پروتکل که نسخه ۲ آن می باشد امروزه مورد استفاده قرار می گیرد.

این امکان وجود دارد که کاربران برای ورود به شبکه از کد کاربری و کلمه عبور استفاده نمایند. این اطلاعات بر روی یک سرور ذخیره می شود و در هنگام ورود کاربر این اطلاعات از روی آن سرور ها مطابقت داده می شود که این مکانیزم ترکیبی با پروتکل های امنیتی که در این بخش ذکر کردیم ؛ انجام می شود.

لیست آدرس های فیزیکی :

شما بر اساس آدرس فیزیکی سیستم های کاربران می توانید به آنها اجازه دسترسی به شبکه را بدهید و یا آنها را از این کار منع نمایید. برای این کار شما لیست آدرس فیزیکی کاربرانی که مجاز به اتصال هستند را وارد نموده و کاربرانی که در این لیست قرار ندارند نمی توانند به شبکه متصل شوند.

غیر فعال کردن نمایش شناسه امنیتی :

اکثر نقاط دسترسی بصورت پیش فرض شناسه امنیتی خود را نمایش می دهند.این امر به این دلیل است که کاربران بتوانند براحتی به شبکه مورد نظر خود را جستجو کرده و به آن متصل شوند. با غیر فعال کردن این گزینه ؛کاربران می بایست اطلاعات مربوط به شبکه را خود وارد نموده و به شبکه دسترسی پیدا نمایند.

حملات امنیتی War driving :

امروزه با کاهش قیمت تجهیزات بیسیم این نوع شبکه ها بسیار پر طرفدار هستند.در بسیاری از شهرهای بزرگ اگر شما در طول خیابان با رایانه خود حرکت نمایید تعداد زیادی شبکه بیسیم را مشاهده خواهید نمود که عمده آنها مربوط به شرکت ها می باشند. در این شهر ها اگر شما با خودرو خود به همراه رایانه در شهر بگردید می توانید تعدادی شبکه بیسیم را پیدا نمایید که فاقد هرگونه تدابیر امنیتی باشند می توانید به راحتی در فاصله ای از شبکه توقف نموده و از منابع آن استفاده نمایید .اتصال به این شبکه ها بدون مجوز خطرات زیادی را به دنبال خواهد داشت. دسترسی به شبکه داخلی و یا استفاده از منابع شبکه یکی از این خطرات است که لزوم استفاده از تدابیر امنیتی در شبکه را بیشتر برای شما روشن می نماید.

افت سیگنال :

یکی دیگر از فاکتور های بسیار مهم در هنگام نصب و راه اندازی شبکه بیسیم افت سیگنال است.این امر به این دلیل اهمیت زیادی دارد که هرچه سیگنال ضعیف تر باشد شبکه غیر قابل اعتماد خواهد بود.فاکتور های دیگری هم در این زمینه موثر هستند که در این بخش به آنها می پردازیم :

فاصله :

این فاکتور بسیار روشن و واضح است. هرچه فاصله شما از نقطه دسترسی بیشتر باشد سیگنال دریافتی ضعیف تر خواهد بود. بسیاری از این تجهیزات فاصله محدودی که معمولا کمتر از ۱۰۰ متر می باشد را پوشش می دهد. برای فواصل بیشتر در یک جهت از انواع آنتن یا تکرار کننده سیگنال استفاده می شود.

دیوار و موانع :

هرچه موانع و دیوارهایی که باید امواج بیسیم از آنها عبور کند بیشتر باشد سیگنال ضغیف تر خواهد شد.البته قطر دیوار ها و موانع بسیار مهم است.هرچه ضخیم تر باشند سیگنال عبوری ضغیف تر خواهد بود بنا براین در محیط های بسته و دارای دیوار و موانع فراوان ممکن است محدوده پوشش شبکه به کمتر از ۱۰ متر تقلیل یابد.

پروتکل مورد استفاده :

یکی دیگر از فاکتورهایی که در محدوده پوشش شبکه بسیار اهمیت دارد پروتکل مورد استفاده در شبکه است. استاندارد های مختلف شبکه بیسیم دارای محدوده پوشش متفاوتی هستند که در مباحث قبلی به آنها پرداخته ایم.

تداخل امواج :

آخرین فاکتوری که بر جریان بی سیم تاثیرگذار است تداخل امواج است. باتوجه به تعاریف اولیه ؛ شبکه وایرلس در باند ۹۰۰ مگا هرتز ودر فرکانس های ۲/۴ یا ۵/۸ گیگا هرتز فعالیت می نماید (برخی تجهیزات غیر استاندارد فرکانس های دیگری هم مورد استفاده قرار می گیرد).

تداخل می تواند توسط منابع مختلفی ایجاد شده باشد این منابع می توانند تلفن های بیسیم ،دستگاه های مایکروویو و یا تلفن همراه و یا بطور کلی توسط هر دستگاهی که امواج رادیویی تولید و ارسال می کند ایجاد شده باشد.

راه اندازی سخت افزار :

نصب تجهیزات سخت افزاری شبکه بیسیم بسیار ساده و آسان است.تجهیزات سخت افزاری ۲ شکل کلی دارند.یا نقطه دسترسی بیسیم هستند و یا کاربر شبکه بیسیم هستند.

نصب کارت شبکه همانند نصب انواع دیگر کارت شبکه است. نصب فیزیکی نقطه دسترسی هم به همین سادگی است کافی است آن را از جعبه خارج نموده ؛آنتن را به آن متصل کرده و در نزدیکترین محل به کاربران قرار دهید. تنها نکته مهم همین نزدیک بودن به کاربران است که باید به آن توجه نمایید. در مکان یابی برای نصب باید دقت نمایید که محل انتخابی شما نسبت به اکثر کاربران نزدیکترین فاصله باشد.این مرحله نیاز به کمی دقت ؛حوصله و سعی دارد.البته برخی مفاهیم مانند این که موانع امواج را تحت الشعاع قرار می دهند هم می تواند خیلی به شما کمک کند. پس از نصب سخت افزاری نوبت به پیکربندی آن می رسد.

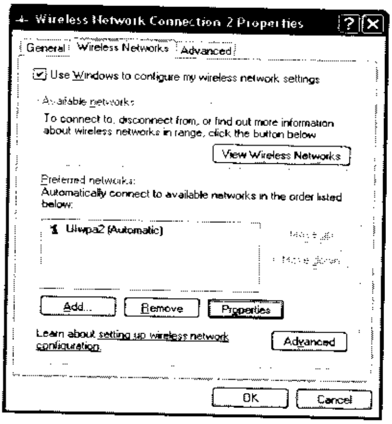
تنظیمات سخت افزاری و نرم افزاری

حال که اجزا ی سخت افزاری نصب شدند باید آنها را پیکر بندی نمود که بتوانند با هم کار کنند.این کار سختی نخواهد بود.زیرا اکثر نقاط دسترسی بیسیم بدون تغییرات با همان تنظیمات اولیه خود هم می توانند فعالیت نمایند.پس بهتر است بگوییم که شما تنظیمات آن را نسبت به شرایط خود تغییر داده و به اصطلاح شخصی سازی می نمایید.

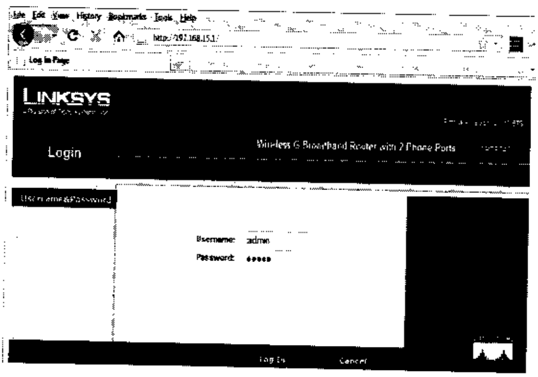
تنظیمات کارت شبکه :

در ویندوز XP نرم افزاری برای تنظیم خودکار ارتباط با شبکه بیسیم پیش بینی شده است.این نرم افزار تمامی شبکه های بیسیم در دسترس را نمایش می دهد و شما می توانید نحوه دسترسی به آنها را مشخص نمایید همچنین تدابیر امنیتی برای ارتباط را هم در این بخش می توانید تنظیم نمایید.

شما می توانید مدیریت ارتباط با شبکه های بیسیم را به ویندوز بسپارید؛ لیست شبکه های بیسیم موجود در دسترس را مشاهده نمایید و به شبکه های توصیه شده توسط ویندوز متصل شوید. این تنظیمات بسیار ساده هستند و شما با کمی دقت می توانید این تنظیمات را به راحتی انجام دهید.



تنظیمات نقطه دسترسی بی سیم :



بطور کلی شاید هزاران نوع و مدل نقطه دسترسی بیسیم هرساله تولید می شود که نحوه پیکربندی آنها با هم تفاوت دارد اما برای پیکربندی می بایست اصول اولیه و پیش شرط های تنظیم را بدانیم . اکثر این تجهیزات از طریق وارد کردن آدرس IP آنها در مرورگر اینترنت پیکربندی می شوند.پس از ورود به صفحه تنظیمات ؛ شما می توانید تمامی تنظیمات مربوط به شبکه و ارتباط بیسیم را تغییر داده و آنها را شخصی سازی نماییم.

برخی پارامترهای مهم در هنگام پیکربندی به این شرح هستند:

SSID (شناسه امنیتی شبکه) : که در مورد آن در مباحث قبلی صحبت کردیم. این شناسه در واقع نام شبکه بیسیم شما خواهدبود.

حالت فعالیت : این دستگاه می تواند در حالت های مختلف مانند پل ارتباطی ،تکرار کننده و مسیریاب فعالیت نماید.شما می توانید حالت مورد نظر را انتخاب نمایید.

کلمه عبور : این کلمه عبور برای ورود به بخش تنظیمات نقطه دسترسی است. تغییر این کلمه عبور اولین اصل در زمان پیکربندی است. زیرا در صورت وروود هر فردی به این بخش تمامی تنظیمات شبکه در دسترس او خواهد بود.

کانال های بیسیم : کلیه تجهیزات بیسیم می توانند در کانال های مختلفی فعالیت نمایند . با تغییر کانال می توان از بروز اختلال و یا تداخل امواج جلوگیری نمود. کانال های مجاز در کشور های مختلف با هم متفاوت بوده و بر اساس قانون آن کشور مشخص می شود.

امنیت : شما می توانید پروتکل امنیتی مورد نظر خود برای امن نمودن ارتباط بیسیم خود را نیز در این بخش معرفی نمایید.در صورت مشخص نمودن پروتکل امنیتی تمامی کاربران شبکه بیسیم هم می بایست این پروتکل را پشتیبانی نموده و آن را برای ارتباط فعال نمایند.

استفاده و یا عدم استفاده از شبکه بیسیم امری است که نیاز به شناخت و دانش کافی در مورد شبکه های سیمی و بیسیم دارد. به عنوان مثال از شبکه بیسیم در مکان های عمومی مانند دانشگاه ها رستورانها ؛ فرودگاه ها و هتل ها امروزه بسیار استفاده می شود.

از شبکه های بیسیم برای مکان هایی با وسعت پوشش زیاد و فراهم نمودن امکان جابجایی برای کاربران شبکه ها استفاده می شود.

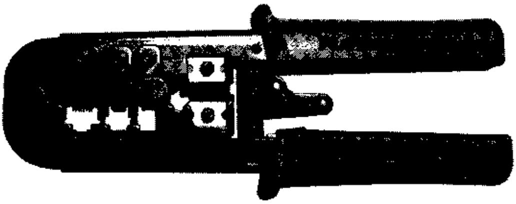
تجهیزات نصب و راه اندازی شبکه

برای اتصال اجزا و راه اندازی یک شبکه ؛ شما نیاز به استفاده از تجهیزات خاصی دارید. این تجهیزات توسط تولید کنندگان معتبر تولید می شود.برخی از این تجهیزات عبارتند از :

- متصل کننده کابل به اتصال

- آزمایش کننده کابل های ارتباطی
- ابزار پانچ و منگنه

متصل کننده کابل به اتصال (Wire Crimping):



این دستگاه را می توان معمولترین ابزار شبکه که آن رادر جعبه ابزار همه کارشناسان شبکه یافت می شود.

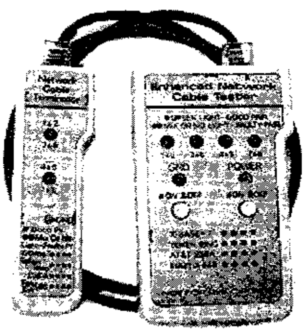
این ابزار برای اضافه کردن اتصال به انتهای کابل برای متصل کردن آن به انواع تجهیزات شبکه بکار می رود.این عمل را Crimping می گویند.انواع اتصالات را در فصل اول آموختیم .برای ساختن یک کابل شبکه ؛ به انتهای کابل شبکه Cat 5 اتصال Rj-45 اضافه می شود و با این وسیله یک کابل شبکه برای اتصال به انواع تجهیزات مانند سویچ و کارت شبکه ایجاد می شود. البته از این ابزار می توان برای تهیه انواع دیگری کابل هم استفاده نمود.

آزمایش کننده کابل های ارتباطی:

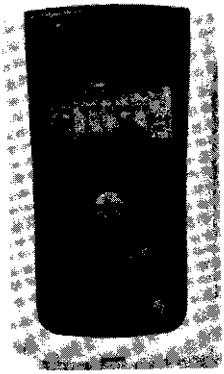
در زمان راه اندازی شبکه و زمان رفع اشکال آن یکی از ابزاری که بیشترین کمک را به شما انجام می دهد ابزارآزمایش کننده کابل های ارتباطی است. با کمک این ابزار شما می توانید به مشکلات کابل ها که اصلی ترین بخش ارتباطی در شبکه های سیمی است پی ببرید و آنها را رفع نمایید.

شما با توجه به نوع کابل ارتباطی یکی از انواع مختلف این ابزار را می توان انتخاب نماییم.انتخاب ابزار مناسب نیاز به شناخت کافی از عملکرد هریک از این ابزار دارد.در این بخش سعی ما بر این است که با عملکرد هریک از این ابزار آشنا شویم.

آزمایش کننده نقشه کابل (Wire Map Testers):

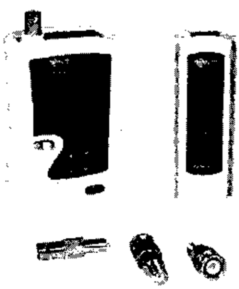


این دستگاه امواج را در طول هر رشته از کابل ها ارسال می نماید تا به سمت دیگرکابل برسد.و وجود هرگونه اشکال در هرکدام از رشته ها را مشخص می نماید.اشکالات پیش آمده می تواند اتصال کوتاه ؛ قطع شدن یک یا چند رشته و یا بروز اشکال در اتصال باشد.



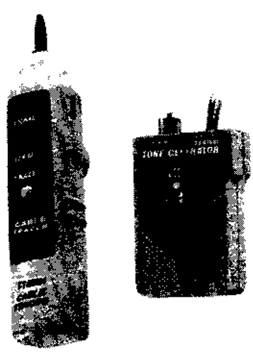
معمولا این تجهیزات به تنهایی گران نیستند اما برخی تجهیزات که برای مقاصد مختلف طراحی شده اند بسیار گران هستند.برخی از این ابزار دارای ۲ بخش هستند بخش اصلی و بخش متحرک که هرکدام در یک سمت کابل قرار می گیرد نتیجه این آزمایش در بخش اصلی نمایش داده می شود. نمایش نتایج آزمایش می تواند به صورت چراغ روشن برای هر رشته سیم که بصورت صحیح متصل شده باشد و یا در انواع گران قیمت تر این ابزار یک بخش هستند و بصورت فعال حتی در صورت اتصال به ابزار شبکه، وضعیت کامل اتصال بر روی صفحه نمایشگر آن نمایش داده می شود.

آزمایش کننده اتصال کابل (Continuity Testers):



این ابزاری است ساده که برای سنجش اتصال در طول کابل بکار می رود. قیمت این ابزار به مراتب ارزانتر از انواع دیگر آزمایش کننده ها می باشد.این ابزار ساده برای شناسایی مشکلات در هنگام راه اندازی شبکه طراحی شده است.این ابزار همانند ابزار قبل از ۲ بخش مجزا تشکیل شده است.

مولد آهنگ (Tone Generators):



این ابزار را می توان ساده ترین ابزار آزمایش و سنجش اتصال کابل شبکه دانست.این ابزار هم از ۲ بخش مجزا تشکیل شده است اما با یک تفاوت و آن که تنها یک سر آن با اتصال Rj-45 به کابل شبکه متصل می شود و سیگنال را در طول کابل منتقل می نماید. بخش دوم آن ابزاری مانند یک قلم است که وقتی به انتهای کابل می رسد یک آهنگ که قابل شنیدن است تولید می نماید.

روند آزمایش با این ابزار بسیار زمانگیر است و شاید زمان آزمایش معادل

زمان اجرای شبکه باشد که این ابزار را نا کارآمد می سازد.همچنین شما باید برای آزمایش تمام طول کابل را طی نمایید که این مرحله باید به ازای هر کابل انجام شود. توجه به این دلایل که در این بخش ذکر شد خرید این ابزار مقرون به صرفه نیست.

تجهیزات آزمایش فیبر نوری (Optical test Set):

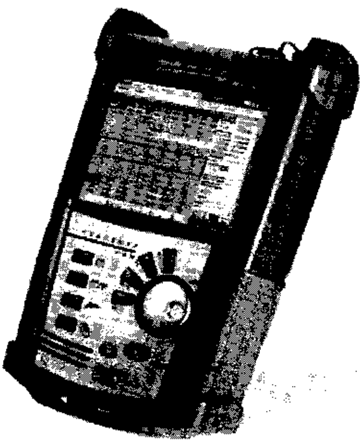
در بسیاری از مواقع ممکن است که شما در یک شبکه هم نیاز به آزمایش کابل های فیبر نوری و هم کابل شبکه پیدا نمایید.در این صورت صرفه اقتصادی بر آن است که شما تجهیزات آزمایشی تهیه کنید که بتواند هر دو شبکه را همزمان آزمایش نماید.



تجهیزاتی که برای آزمایش فیبر نوری بکار می روند OLTS(Optical Loss Test Set) نامیده می شود.البته از این تجهیزات نمی توان برای تست میدانی و در محل نصب استفاده نمود زیرا این ابزار برخلاف ابزار آزمایش دیگر از یک بخش تشکیل شده است.یعنی برای آزمایش یک فیبر نوری نیاز به ۲ دستگاه در ۲ طرف می باشد.

البته برخی دستگاه های پیشرفته تر و همچنین گران تر وجود دارند که می توان با کمک ابزار کمکی آنها تمامی انواع کابل های شبکه و فیبر نوری را آزمایش نمود که در بخش بعدی به آنها خواهیم پرداخت.

ابزار آزمایش چند کاره (Multi Functioning Testers) :



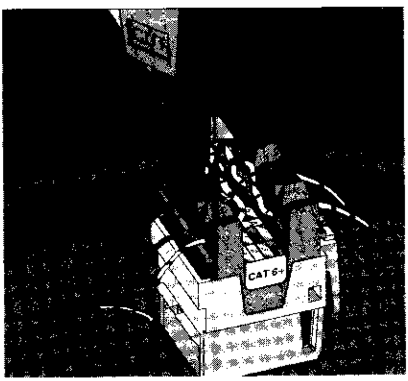
با پیشرفت تکنولوژی و همچنین گسترده شدن ابزار ارتباط و رسانه ای ،ابزارهای آزمایشی که امروزه بیشتر به فروش می رود از این دسته ابزار هستند.این ابزار هم برای آزمایش کابل های مسی و هم کابل های فیبر نوری مورد استفاده قرار می گیرد.

یکی از مزایای این ابزار آن است که هر کسی می تواند آزمایش را انجام دهید.فقط کافی است کابل را به آن متصل نموده و کلید مربوط به آزمایش را فشار دهید ؛ نتیجه آزمایش بر روی صفحه نمایش

ظاهر خواهد شد. همچنین می توان نتایج آزمایش ها را بر روی حافظه دستگاه ذخیره نمود و سپس نتایج را به رایانه منتقل نمود و یا آنها را چاپ نمود.

البته ممکن است سادگی کاربرد یکی از معایب این ابزار هم باشد زیرا شما نمی دانید که در هنگام انجام آزمایش دقیقا چه اتفاقاتی می افتد و شما می بایست کاملا به شرکت سازنده ابزار اعتماد نموده و نتیجه تست را بپذیرید. برای جلوگیری از بروز خطا و همچنین بروز رسانی جهت پشتیبانی از استاندارد ها و تجهیزات جدید شرکتهای سازنده این ابزار ها زمانی را برای بررسی و بروز رسانی اختصاص می دهند که نتایج ارایه شده توسط دستگاه همیشه صحیح باشد.

ابزار منگنه یا پانچ (Punchdown Tools) :



امروزه اکثر شبکه ها توسط کابل های شبکه UTP راه اندازی می شود. یک سمت این کابل ها به ترمینال کابل ها متصل می شود. اتصال کابل ها به ترمینال توسط ابزار پانچ انجام می شود. شکل روبرو نحوه انجام این کار را برای شما نمایش می دهد.



ابزاری که عمل پانچ را انجام میدهد ابزاری مشابه شکل روبرو است که به نسبت عملکردش امکان تغییر تیغه را دارد که هر تیغه می تواند کار خاصی را انجام دهد این ابزار عمل پانچ و قطع سیم اضافه را همزمان انجام می دهد.

جمع بندی:

در این بخش شما:

- **با خصوصیات اختصاصی مانند سرعت انتقال ؛فرکانس ؛ نحوه انتقال و توپولوژی در شبکه های بیسیم آشنا شدید**
- **با فاکتور هایی که بر فاصله و سرعت شبکه های بیسیم تاثیر دارد مانند تداخل فرکانس و موانع فیزیکی آشنا شدید.**
- **درخصوص ابزار های سنجش ارتباط در شبکه های سیمی مطالب مهمی آموختید.**
- **درخصوص انواه استاندارد ها و تجهیزات فیزیکی کاربردی در شبکه های بیسیم مطالب مهمی آموختید.**

سوالات ارزیابی برای آزمون Network+ :

۱ –کدام نرم افزار ارتباط سیستم عامل با کارت شبکه را بر قرار می کند.

الف) پروتکل ارتباطی

ب) نرم افزار کارت شبکه

ج) سیستم عامل

د) نرم افزار سیستم

۲-کدامیک از این آنتن ها فاصله طولانی تری را پوشش می دهد.

الف) آنتن همه جهته با قدرت 7dBi

ب) آنتن تک جهته با قدرت 7dBi

ج) آنتن همه جهته با قدرت 8dBi

د) آنتن تک جهته با قدرت 8dBi

۳-کدامیک از موارد زیر هویت و نام یک شبکه بیسیم را مشخص می نماید.

الف) Network ID

ب) آدرس MAC

ج) NIC

د) SSID

۴- برای تهیه یک کابل شبکه به متراژ ۲۰ متر کدامیک از این ابزار مورد استفاده قرار می گیرد.

الف) ابزار پانچ

ب) متصل کننده کابل به اتصال

ج) آزمایش کننده کابل های ارتباطی

د) ابزار منگنه کابل

۵-کدامیک از این پدیده ها در زمان افت ولتاژ اتفاق می افتد. (تمامی موارد صحیح را مشخص نمایید)

الف) ضعیف شدن ناگهانی(sag)

ب) ضعیف شدن طولانی(Brownout)

ج) کنترل کننده افزایش موجی (Surge Protector)

د) قطع جریان (Blackout)

۶- کدامیک فرمول برای تبدیل dBi بهdBd صحیح است .

الف)dBi =2.2 + dBd

ب) dBi =2.2 x dBd

ج) dBd=2.2 + dBi

د) dBd =2.2 x dBi

۷- در کدام ساختار کاربران شبکه بیسیم میتوانند بدون وجود نقطه دسترسی بیسیم با هم در ارتباط باشند.

الف)حالت زیر ساخت

ب) استاندارد Wi-Fi

ج) حالت Ad-Hoc

د) استاندارد 802.11 b

۸- حد اکثر سرعت انتقال مربوط به کدام استاندارد شبکه های بیسیم است.

الف) استاندارد 802.11 a

ب) استاندارد 802.11 b

ج) استاندارد 802.11 g

د) استاندارد 802.11 n

۹- ارتقای نرم افزار یک کارت شبکه بیسیم می تواند باعث بروز کدامیک از این اتفاقات باشد . (تمامی موارد صحیح را مشخص نمایید)

الف) سرعت شبکه بیسیم را افزایش می دهد.

ب) امکان پشتیبانی از استاندار 802.11 n را به آن اضافه می کند.

ج) مشکلات نرم افزاری را برطرف می نماید.

د) می تواند قدرت دریافت داده ها را افزایش دهد.

۱۰- کدامیک از این استاندارد ها در فرکانس 5GHZ فعالیت می نماید.

الف) استاندارد 802.11 n

ب) استاندارد 802.11 g

ج) استاندارد 802.11 b

د) استاندارد 802.11 a

پاسخ به سوالات این بخش

۱ - **ب**

نرم افزار کارت شبکه وظیفه تعامل و برقراری ارتباط با سیستم عامل را برعهده دارد.

۲ - **د**

آنتن تک جهته قدرت را در یک جهت جمع می نماید و می تواند مسافت بیشتری را پوشش دهد اما سطح زیر پوشش آنتن همه جهته بسیار بیشتر است.

۳ - **د**

SSID هویت و شناسه امنیتی هر شبکه است که برای راهنمایی کاربران بکار می رود.

۴ - **ب**

برای تهیه کابل شبکه از ابزار متصل کننده اتصال به کابل یا Wire Crimping استفاده می شود.در صورت بروز مشکل از ابزار سنجش استفاده می شود.

۵ - **الف ، ب ،د**

گزینه ج یا کنترل کننده افزایش موجی یک دستگاه است که می تواند امواج الکتریکی ورودی را کنترل کند.

۶ - **الف**

طبق مطالب این بخش فرمول صحیحdB i =2.2 + dBd می باشد.

۷ - **ج**

تنها در این ساختار ارتباط بصورت مستقیم برقرار می شود و نیاز به ارتباط از طریق سیستم مرکزی نمی باشد.

۸ - **د**

بیشترین سرعت مربوط به استاندارد 802.11 n بوده و سرعت در این حالت ۳۰۰ مگابیت در ثانیه است.

۹ - **ج**

سرعت شبکه بیسیم تنها با ارتقای نرم افزاری افزایش نمی یابد.افزوده شدن امکان پشتیبانی از یک استاندارد نیاز به ارتقای سخت افزاری هم دارد. قدرت دیافت یا ارسال داده ها بیشتر به قدرت فیزیکی بستگی دارد.

۱۰ - **الف**

تنها استاندارد استاندارد 802.11 a در فرکانس 5GHZ فعالیت می نماید و بقیه درفرکانس 2.4GHZ هستند.

فصل هفتم

تکنولوژی شبکه های وسیع و راه دور



شما در این فصل با این مفاهیم آشنا خواهید شد:

۷-۱ شناسایی خصوصیات کلی مانند : سرعت ،ظرفیت و نحوه انتقال و در شبکه های با مقیاس وسیع:

- بسته ها
- مدارها
- ISDN
- FDDI
- T1,E1,J1
- T3,E3,J3
- OC-x
- X.25

۷-۲ آشنایی با خصوصیات تکنولوژی های ارتباط با شبکه اینترنت مانند :

- ارتباط xDSL
- مودم کابلی
- شبکه های POTS/PSTN
- بیسیم
- ماهواره

۶-۳ شناسایی عملکرد تکنولوژی های دسترسی راه دور مانند:

- سرویس دسترسی راه دور
RAS(Remote Access Protocol)
- پروتکل ارتباط نقطه به نقطه

PPP(Point To Point Protocol)

- ❖ پروتکل ارتباط مستقیم به اینترنت SLIP(Serial Line Internet Protocol)
- ❖ پروتکل ارتباط نقطه به نقطه بر روی بستر اینترنت

  PPOE(Point To Point Protocol Over Ethernet)
- ❖ پروتکل تونل در ارتباط نقطه به نقطه

  PPTP(Point To Point Tunneling Protocol)
- ❖ شبکه مجازی خصوصی

  VPN(Virtual Private Network)
- ❖ پروتکل صفحه کاری راه دور

  RDP(Remote Desktop Protocol)



۷- ۴ اجرای یک ارتباط راه دور و بررسی نحوه تصدیق ورود در سیستم عامل های مختلف مانند:

- ❖ یونیکس/لینوکس و مکینتاش
- ❖ ناول
- ❖ ویندوز
- ❖ سیستم عامل Apple Share IP

مقدمه:

تکنولوژی های دسترسی راه دور به کاربران اجازه می دهد که به شبکه شما متصل شده واز رایانه ای خارج از شبکه از منابع و سرویس های آن استفاده نمایند.در طول سال های اخیر نیاز به دسترسیاز راه دور به رایانه های درون شبکه زیاد شده است.ممکن است شما در طول یک سفر تجاری نیاز داشته باشید که همیشه به رایانه خود و منابع درون شبکه ارتباط داشته باشید و یا عملکرد کارکنان بخش خود رابررسی نماییدتمامی این اقدامات با کمک پروتکل های دسترسی راه دور امکان پذیر شده است.

برای برقرای ارتباط راه دور هر دو سمت ارتباط می بایست برای این کار پیکربندی شده باشند.این کار نیاز به برخی نرم افزار و سخت افزار خاصی دارد که باید تهیه شود.برقرای این ارتباط برای تمامی مدیران شبکه تمامی کسانی که می خواهند در آزمون Network+ شرکت نمایند لازم است.

پیش نیاز های برقرای ارتباط راه دور

برقراری ارتباط راه دور نیاز به ۲ جزء اصلی دارد که عبارتند از : سیستم راه دور و سیتم برقرار کننده ارتباط راه دور در شبکه که معمولا آن را سرور دسترسی راه دور می نامند. کاربر راه دور به سرور درون شبکه متصل می شود و پس از آن به عنوان یک کاربر درون شبکه عمل می نماید.

در این بخش تنها به یکی از انواع دسترسی راه دور می پردازیم.این نوع ارتباط ارتباط از طریق خطوط تلفن آنالوگ می باشد. البته امکانات و تنظیمات مربوط به این ارتباط در سیتم عامل های مختلف متفاوت هستند. برای آشنایی با امکانات هر سیستم عامل باید به راهنمای تنظیمات همان سیستم عامل مراجعه نمایید.

در بخش بعدی شما با نیاز های نرم افزاری و سخت افزاری برای برقرای ارتباط راه دور بوسیله مودم و خطوط تلفن آنالوگ آشنا می شوید.

نیاز های سخت افزاری

دستگاهی که برای برقرای ارتباط رایانه از طریق شبکه تلفن عمومی استفاده می شود مودم نامیده می شود. مودم در واقع مبدلی است برای تبدیل سیگنال های آنالوگ به دیجیتال و برعکس.

در زمان ارسال مودم سیگنال های دیجیتال رایانه را به آنالوگ تبدیل می نماید تا بر روی خطوط آنالوگ منتقل شود و در زمان دریافت امواج آنالوگ را به دیجیتال تبدیل می نماید.از آنجا که خطوط تلفن را تقریبا در همه جا می توان پیدا کرد ، این روش را می توان معمولترین روش برای دسترسی راه دور دانست.

تبدیل دیجیتال به آنالوگ در واقع تبدیل داده های دیجیتال به ۰ و ۱ است که بتواند بر روی شبکه آنالوگ منتقل شود. این روش سرعت انتقال داده ها رادر مقایسه با انتقال بصورت دیجیتال بسیار کاهش می دهد اما می تواند داده ها را در مسافتی طولانی تر ارسال نماید.

مودم می تواند داخلی و یا خارجی باشد.فرق اصلی آنها در نوع تنظیمات آن ها ست.مودم های داخلی تنظیمات متفاوتی مانند IRQ ؛آدرس ورودی /خروجی (I/O) ودرگاه COM را نیاز دارد اما مودم خارجی تنها نیاز به اتصال به رایانه دارد و با نصب نرم افزار می تواند شروع به کار نماید.آدرس درگاه های مورد استفاده در این تجهیزات در جدول زیر آمده است .لازم است که این آدرس ها را به خاطر بسپارید.

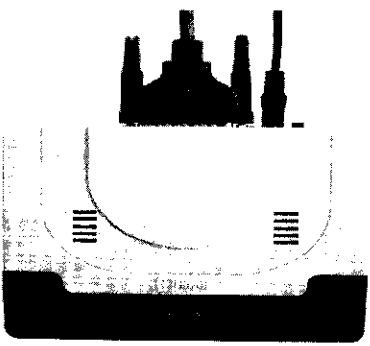
درگاه (پورت)	IRQ	آدرس I/O
Com1	4	3F8
Com2	3	2F8
Com3	4	3E8
Com4	3	2E8

تنظیمات مودم داخلی



مودم های داخلی ؛ در واقع یک کارت افزودنی هستند که به کامپیوتر اضافه می شود. این ابزار پس از نصب و پیکربندی امکان اتصال به شبکه را فراهم می نماید. نصب و پیکر بندی این کارت تقریبا شبیه نصب هر کارت افزودنی دیگر است .

تنظیمات مودم خارجی



اگرچه اکثر مودم هایی که امروزه مورد استفاده می شود مودم های داخلی هستند اما در موارد خاصی ضرورت پیدا می کند که شما از مودم های خارجی استفاده نمایید.

برخی افراد ترجیح می دهند که از مودم خارجی استفاده نمایند تا در هر حالتی بتوانند چراغ وضعیت مودم را مشاهده نمایند.اگرچه چراغ وضعیت در مودم های داخلی هم وجود دارد اما مشاهده آن برای کاربران کمی دشوار خواهد بود.

برای نصب این مودم ها شما باید به این موارد دقت نمایید : درگاه یا پورت سریال و یکی از انواع UART

درگاه های سریال

با افزایش تعداد دستگاه هایی که از پورت سریال استفاده می نمایند مانند مودم ها ,دوربین و چاپگر ها در برخی موارد پورت سریال آزاد برای استفاده وجود ندارد.برای رفع این مشکل درگاه جدیدی با نام USB مورد استفاده قرار می گیرد. از هرپورت می توان برای اتصال حداکثر ۱۲۷ دستگاه به کامپیوتر استفاده نمود.

انواع UART

UART مخفف عبارت Universal Asynchronus Receiver-transceiver می باشد که در واقع یک تراشه است که برای مدیریت تبادل داده های پورت سریال مورد استفاده می گیرد.هر تراشه سرعت تبادل داده ها در هر پورت سریال را مشخص می نماید. در حال حاضر دو سری تراشه وجود دارد.سری ۸۲۵۰ و ۱۶۵۵۰

سری ۸۲۵۰ می تواند حداکثر سرعتی معادل ۹۶۰۰ بایت در ثانیه را مدیریت نماید. این تراشه ها تا قبل از سال ۱۹۸۶ توسط شرکت های سازنده سخت افزار مورد استفاده قرار می گرفت.

در سری ۱۶۵۵۰ سرعت انتقال به ۱۱۵۲۰۰ بایت در ثانیه ارتقا یافت و جایگزین سری های قدیمی گردید.

نیاز های نرم افزاری

پس از بررسی نیاز های سخت افزاری و تنظیمات مودم ؛ می بایست تنظیمات نرم افزاری در سیستم عامل را هم مورد بررسی قرار می دهیم.در این بخش تنظیمات نرم افزاری مودم در سیستم عامل ویندوز ۲۰۰۰ را مورد بررسی قرار می دهیم.

برای تنظیمات می بایست به کنترل پنل و بخش تنظیمات سخت افزار وارد شویم در این بخش تنظیمات مربوط به مودم را می توان تغییر داد.

به علاوه شما می بایست نرم افزار مورد نظر برای مدیریت اتصال را هم تنظیم نمایید.از این نرم افزار برای مدیریت اتصال مودم به سیستم راه دور وکمک گرفتن از پروتکل های مختلف برای این اتصال استفاده می شود.

- پروتکل TCP/IP
- پروتکل IPX
- پروتکل PPP
- پروتکل PPTP
- پروتکل L2TP

ارتباط تنها زمانی برقرار می گردد که هر دو تنظیم سخت افزاری و نرم افزاری به درستی تنظیم شده باشد.

روش های دسترسی راه دور

از آنجا که سیستم راه دوری که شما می خواهید به آن متصل شوید در داخل شبکه شما نیست اتصال شما از طریق تکنولوژی های شبکه محلی نیست و به جای آن از روش ها و تکنولوژی های دیگری استفاده می نماید در این بخش به برخی از آنها اشاره می نماییم :

- سرویس های تلفن عمومی (PSTN(Public Switched Telephone Network
- شبکه دیجیتال (ISDN(Integrated Service Digital Network
- سایر اتصال های دیجیتال مانند شبکه های DSL و اتصالات باند پهن و اتصالات سری E و T

شبکه های تلفن شهری (PSTN(Public Switched Telephone Network

گستره این شبکه در تمامی نقاط دنیاست ؛ این شبکه را شبکه قدیمی تلفن هم می توان دانست.این تکنولوژی همه گیر ترین روش برای اتصال راه دور به دلیل قیمت پایین این اتصال؛ سهولت کاربرد و تنظیمات است.

در این شبکه ها دو نکته بسیار اهمیت دارد: شبکه عمومی و سوییچ

شبکه عمومی درست در مقابل شبکه خصوصی است که منظور همان کابل کشی در سطح شهر و محدوده پوشش شبکه است که هر مشترک می تواند از مزایای این شبکه بهره مند گردد.و سوییچ بیانگر نحوه عملکرد سیستم تلفن است.

در این شبکه ممکن است شما چندین زوج سیم در حالت رزرو داشته باشید که در زمان نیاز بتوان برای اتصال از آن استفاده نمود.

برای بیشتر روشن شدن این مبحث یک مثال مطرح می نماییم.البته لازم است پیش از آن توضیحی در مورد سیستم شماره تلفن ارایه نماییم.نحوه اختصاص شماره و شماره گیری در کشور های مختلف با هم متفاوت است اما تکنولوژی برقراری ارتباط و شماره گیری در همه جا یکسان است.

شرکت تلفن برای هر مشترک یک زوج سیم مسی از مرکز تلفن که به آن (CO) می گویند تا محل کار یا زندگی مشترک برقرار می نمایند.تمامی کابل های مشترکین در مرکز تلفن جمع می گردد.در این مرکز تجهیزات خاصی وجود دارد که به آن سوییچ می گویند.در واقع عملکرد این دستگاه شبیه عملکرد همان سوییچی است که در فصل دوم در مورد آن صحبت نمودیم.سوییچ وظیفه برقراری تماس و حفظ آن تا زمانی که کاربران اقدام به قطع ارتباط ننمایند را برعهده دارد. در هر سوییچ یک سمت به شبکه تلفن محلی و سمت دیگر آن از طریق چندین سوییچ به تلفن مخاطب مرتبط می شود که تعداد این سوییچ ها تا مقصد بستگی به فاصله دارد.

برای برقراری یک تماس شما گوشی را بر می دارید؛ این کار چرخه را کامل می کند و شما بوق خط را می شنوید این بوق در واقع اعلام آمادگی سوییچ برای برقراری ارتباط است.در زمان وجود اشکال در برقراری

ارتباط شما بوق دیگری را می شنوید که بیانگر وجود اختلال در ارتباط است. هنگام نیاز سنجی برای سوییچ تلفن معمولا درصدی از تعداد کاربران را مد نظر قرار می دهند یعنی امکان برقراری ارتباط همزمان برای همه کاربران وجود نخواهد داشت و تنها معمولا ۶۰ تا ۸۰ درصد ظرفیت مورد نظر قرار می گیرد زیرا سوییچ های مخابراتی بسیار گران هستند و این کار برای پایین آوردن هزینه تلفن بسیار مهم است.

بر اساس تکنولوژی های ارتباط راه دور ؛ این شیوه مزیت هایی دارد که به این شرح می باشد :

- این روش ارزان است.تقریبا در اکثر خانه ها خط تلفن وجود دارد.
- هزینه کابل کشی برای شبکه محلی وجود ندارد.
- ارتباط تلفنی بین اکثر کشور های دنیا وجود دارد.

این روش معمولترین روش ارتباط راه دور است زیرا معایب بسیار کمی دارد.اما برخی معایب آن هم در این بخش معرفی می گردد :

- پهنای باند محدودی دارد.
- میزان تبادل داده ها در این روش به دلیل تبادل از طریق سیستم آنالوگ در مقایسه با روش دیجیتال محدود است. ارتباط در این حالت در بهترین شرایط می تواند حداکثر به ۵۶ مگابیت در ثانیه برسد.

شبکه های دیجیتال(ISDN(Integrated Service Digital Network

شبکه ISDNیک شبکه نقطه به نقطه دیجیتال است که می تواند تا ۲ مگابیت در ثانیه را منتقل نماید البته برای انتقال از ۲ نوع خط استفاده می شود در خطوط PRI میزان انتقال ۲ مگابیت در ثانیه و در خطوط BRI این میزان ۱۲۸ کیلو بیت در ثانیه می باشد. که در این بخش ما هرجا سخن از ISDN می نماییم منظورمان خطوط BRI می باشد.

با توجه به برخی مولفه ها مانند سرعت بالا و هزینه اندک این روش هم یکی از روش های معمول برای ارتباط راه دور به حساب می آید.این خطوط از همان کابل هایی که در شبکه های تلفن شهری استفاده می نمایند اما تفاوت آنها در این نکته است که در این خطوط صدا بصورت دیجیتال منتقل می شوند که این امر تفاوت های زیادی را ایجاد می نماید که در این بخش در مورد آنها صحبت می نماییم.

برای اتصال این شبکه ها دستگاهی به نام آداپتور ترمینال استفاده می شود که برخی به اشتباه به آن مودم ISDN میگویند.لفظ مودم از این رو اشتباه است زیرا هیچ تبدیلی از آنالوگ به دیجیتال انجام نمی شود بلکه تنها داده های دیجیتال را منتقل می کند.

خطوط دیجیتال دارای دونوع کانال هستند.داده ها در کانال های ویژه ای به نام کانال B منتقل می شوند .هرخط BRIدارای ۲ کانال Bاست که هرکدام می تواند ۶۴ کیلوبیت داده را منتقل نمایند.نوع دیگر کانال ؛

کانال D است که داده های مربوط به مدیریت اتصال و تنظیمات اتصال را منتقل می نمایند.این کانال پهنای باندی معادل ۱۶ کیلوبیت در ثانیه دارد.

برای انتقال داده ها با پهنای باندی معادل ۱۲۸ کیلوبیت در ثانیه هردو کانال B رابصورت یک کانال واحد در نظر می گیرند به این حالت Binding می گویند. در این حالت هم کانال D برای انتقال تنظیمات استفاده می شود.

برخی مزایای این نوع شبکه عبارتند از :

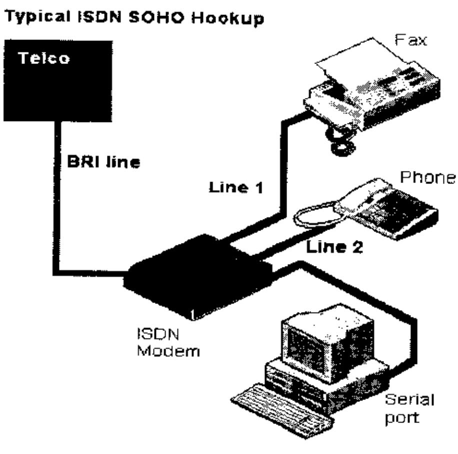
- ارتباطی سریع است.
- پهنای باندی معادل ۱۲۸ کیلوبیت در ثانیه دارد.
- هیچگونه تبدیلی بین آنالوگ و دیجیتال انجام نمی شود

به علاوه خطوط دیجیتال معایب اندکی هم دارند که عبارتند از :

- گرانتر از خطوط آنالوگ هستند.
- تجهیزات ویژه ای در سمت کاربر و شرکت تلفن نیاز دارد.
- تجهیزات مربوط به این خطوط امکان برقراری ارتباط با خطوط دیگر را ندارند.
- این نوع ارتباط نیاز به برقراری ارتباط دارندازاین رو ارتباط دایمی نیست.

> در هنگام کار با خطوط تلفن باید همیشه احتیاط کنید زیرا خطوط تلفن معمولا حاوی جریان الکتریکی است که ممکن است به شما صدمه بزنند.

در تصویر ساختار یک شبکه ISDN را مشاهده می نمایید.



انواع دیگر خطوط دیجیتال

خطوط دیجیتال امکان دریافت پهنای بیشتر نسبت به تکنولوژی های قدیمی تر را فراهم آوردند.برخی دیگر از خطوط دیجیتال عبارتند از :

- xDSL
- مودم کابلی
- Frame Relay
- سری T
- خطوط ATM
- خطوط فیبر نوری

تکنولوژی xDSL :

این تکنولوژی یکی از تکنولوژی هایی است که از بستر کابل مسی برای انتقال داده ها استفاده می نماید.به دلیل استفاده از سیستم تلفن شهری بسیار ارزان است. از این رو امروزه بسیار معمول و پر طرفدار می باشد.در این ساختار شما با هزینه ای بسیار کمتر از یک خط اختصاصی مانند (T1) می توانید از این ساختار استفاده نمایید.

برخی از این شبکه ها عبارتند از :

- HDSL(High-Data-Rate DSL) : این ساختار برای انتقال داده ها با نرخ انتقال بالا مورد استفاده قرار می گیرد
- SDSL(Single Line DSL): در این ساختار از یک سیم برای انتقال داده ها استفاده می شود.
- VDSL: (Very High Data-rate Digital Subscriber Line) برای تبادل داه ها با سرعت بسیار بالا استفاده می شود
- ADSL : (Assymmetric Digital Subscriber Line) معمولترین ساختار تکنولوژی DSLاست

ADSL امروزه فراگیر ترین ساختار تکنولوژی DSL به شمار می رود .حجم بالای داده ها که در این تکنولوژی منتقل می شود به کاربران اجازه می دهدتا داده هایی از جنس های مختلف مانند تصویر , صدا و حتی فیلم را بر روی این بستر منتقل نمایند.نکته بسیار جالب در این تکنولوژی استفاده همزمان از تلفن و ADSL است .برای این کار از دستگاه جدا کننده امواج صوت و داده که به آن جداکننده یا اسپلیتر (Splitter) می گویند؛ استفاده می شود.این تکنولوژی برای کاربران عمومی ایده آل است.

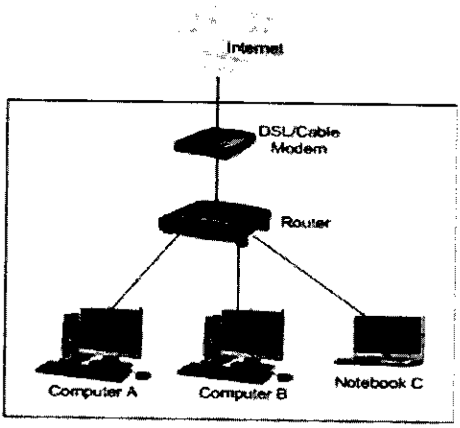
در تمامی ارتباطات DSL نیاز به یک مودم در همه مشترک است.البته هر مودم تنها در ساختار مربروط به خود قابل استفاده خواهد بود.

شبکه های کابلی با مودم کابلی (Cable Modem)

یکی دیگر از روشهای برقراری ارتباط راه دور استفاده از مودم کابلی است. در این روش داده ها از طریق کابل تلویزیون منتقل می شود.در شهرهایی که تلویزیون کابلی رواج دارد مقرون به صرفه ترین روش دسترسی به اینترنت پرسرعت است.در این روش امواج تلویزیونی و داده ها بر روی کابل تلویزیون منتقل می شوند. در سمت کاربر یک مودم قرار می گیرد که مدیریت ارتباط را بر عهده دارد.ارتباط مودم با رایانه کاربران می تواند از طریق پورت USB و یا اترنت و یا هردو اتصال باشد.

در صورتی که تعداد کاربرانی که از این شبکه استفاده می نمایند زیاد تر باشد می توان از یک هاب یا سوییچ استفاده نمود.

در شکل زیر می توان ساختار کلی شبکه مودم کابلی را مشاهده نمایید.



تکنولوژی Frame Relay :

این تکنولوژی یکی از ساختار های شبکه های وسیع است که می تواند بسته هایی با اندازه های متفاوت را بر روی شبکه منتقل نماید.در این روش داده ها در سمت فرستنده به بخش های کوچکتری تقسیم می شوند که از طریق سوییچ های شبکه منتقل می شوند.هر داده در شبکه از مسیریاب های متفاوتی برای رسیدن به مقصد عبور می نماید.سپس در مقصد این داده ها طبق روال اولیه سرهم می شوندتا داده ها به شکل اول تبدیل شوند.

این ساختار داده ها از طریق یک مدار مجازی (PVC :Permanent Virtual Circuit)منتقل می شوند PVC امکان انتقال داده ها از طریق یک مدار مجازی از سمت فرستنده به گیرنده را فراهم می آورد.این ساختار تضمین می کند که داده هایی که از یک سمت وارد این چرخه می شوند از سمت دیگر از طریق یک ارتباط مشابه به درستی خارج می شوند.

یکی دیگر از مزایای استفاده از سیستم های اشتراکی این است که در برخی موارد شما از پهنای باند بیشتری از آنکه شما سفارش داده و مبلغ آن را پرداخت کرده اید استفاده می نمایید. در این شبکه ها شما پهنای باند و ترافیک خاصی را انتخاب می نمایید و هزینه آن را برای مدت معینی پرداخت می نمایید.

ارتباطات سری T :

اتصالات سری T از انواع خطوط دیجیتال است که شما می توانید آن راهمانند یک خط تلفن عمومی از شرکت تلفن اجاره نمایید. در این ساختار از تقسیم زمان چندگانه برای تقسیم پهنای باند به کانال های مختلف جهت انتقال استفاده می نماید. برای نمایش ساختار های مختلف این تکنولوژی در کنار T یک عدد نمایش داده می شود.هر ساختار در سرعت و تعداد کانال با هم متفاوت هستند. در جدول زیر ساختار های متفاوت این خطوط را مشاهده می نمایید:

نوع خط	حداکثر سرعت
T1	1.544 مگابیت در ثانیه
T1C	3.152 مگابیت در ثانیه
T2	6.312 مگابیت در ثانیه
T3	44.736 مگابیت در ثانیه
T4	274.176 مگابیت در ثانیه

خطوط T1:

ارتباط T1یکی از انواع خطوط دیجیتال است که می تواند ۱.۵۴۴ مگابیت در ثانیه را بر روی یک زوج سیم مسی منتقل نماید.این خطوط می توانند برای انتقال صوت یا دیتا بصورت دیجیتال مورد استفاده قرار گیرند. همچنین می توان تلفن های آنالوگ را در مسافت های طولانی بر روی این بستر به دلیل کیفیت و همچنین استفاده از سیگنال دیجیتال منتقل نمود. این روش داده ها و صوت جدا می شونداین مزیت به شرکت ها این امکان را می دهد تا بر روی یک زوج سیم ؛ تلفن و داده های خود را منتقل نمایند و نیازی به سیم کشی مجزا نداشته باشند.

> نسخه اروپایی خطوط T1با نام E1 معرفی می شود.در این خطوط سرعت انتقال داده ها ۲/۰۴۸ مگابیت در ثانیه می باشد. همچنین شاید شما در مورد خطوط J1 هم شنیده باشید.این نسخه ژاپنی این خطوط است که همانندT1 بوده و میزان انتقال داده ها ۱/۵۴۴ مگابیت در ثانیه می باشد.

چه خطی برای ما مناسب است؟

شما برای استفاده از شبکه اینترنت یکی از انواع خطوط دیجیتال را می بایست انتخاب نمایید.این انتخاب بر مبنای میزان استفاده شرکت یا سازمان از اینترنت است.ممکن است هزینه یک خط T1برای یک مجموعه زیاد باشد اما برای یک مجموعه دیگر حتی یک خط T4هم نیازهای شبکه را برطرف نمی نماید.

خطوط T3 :

عملکرد خطوط T3 بسیار شبیه خطوط T1 است با این تفاوت که میزان انتقال داده ها در این خطوط تقریبا ۲۸ برابر خطوط T1 است. این خطوط بر روی بستر فیبر نوری منتقل می شوند.معمولا اکثر سرویس دهنده های اینترنت برای دریافت دیتا و خطوط تلفن از این خطوط استفاده می نمایند.به علاوه شرکت های بزرگ بین المللی برای ارتباط بین دفاتر مختلف خود از این خطوط استفاده می نمایند.

نسخه اروپایی خطوط T3 با نام E3 معرفی می شود.در این خطوط سرعت انتقال داده ها ۳۴/۳۶۸ مگابیت در ثانیه می باشد. J3 نسخه ژاپنی این خطوط است میزان انتقال داده ها ۳۲/۰۶۴ مگابیت در ثانیه می باشد.

خطوط ATM:

خطوط ATM(Asynchronous Transfer Mode) برای انتقال داده ها با سرعت زیاد طراحی شده بود که به هیچ کدام از تکنولوژی های شبکه های محلی وابسته نیست.در این ساختار داده ها و یا صوت می تواند بصورت کاملا همزمان بدون تاخیر زمانی منتقل شوند. داده ها در این روش به بخش های کوچکتری به نام سلول که هرکدام ۵۳ بایت هستند تقسیم می شود.در این روش حجم سلول ها کاملا ثابت هستند اما طول فریم ها متغیر است.

در این ساختار داده ها بسیار سریع در شبکه منتقل می شود.برای این کار بین فرستنده و گیرنده یک ارتباط مجازی ایجاد می نماید تا داده ها به راحتی و بسیار سریع منتقل گردد.هر داده در راه خود تا رسیدن به مقصد از سوییچ های فراوانی عبور می نماید اما ترتیب داده ها رعایت می شود و تنها پس از رسیدن سلول اول به مقصد سلول دوم ارسال می گردد.پس از اتمام عملیات انتقال بر اساس ترتیب اولیه داده ها سرهم بندی می شوند تا به شکل داده اولیه در آیند.

میزان انتقال داده ها در این ساختار بسیار انعطاف پذیر است و می تواند از سرعتی در حد ۱/۵ مگابیت در ثانیه شروع شده و و سرعت انتقال ۲۵ مگابیت در ثانیه ؛۵۱ مگابیت در ثانیه؛۱۰۰ مگابیت در ثانیه و ۱۵۵ مگابیت در ثانیه

و بالاتر را منتقل نماید.رسانه در این انتقال می تواند فیبر نوری یا زوج سیم مسی باشد. البته برای انتقال با سرعت های بالا استفاده از فیبر نوری توصیه می گردد.سرعت های معمول در این ساختار ۵۱/۸۴ و ۱۵۵/۵۲ مگابیت در ثانیه می باشند که می توانند بر روی هر دو بستر فیبر نوری یا سیم مسی معمولی منتقل شوند.اما سرعتی برابر با ۶۲۲/۰۸ مگابیت در ثانیه هم امروزه بسیار مورد استفاده قرار می گیرد تنها بر روی بستر فیبر نوری قابل انتقال می باشد.

در آمریکا استاندارد انتقال داده هابصورت متقارن بر روی بستر فیبر نوری بر اساس استاندارد (SONET) مشخص می گردد .معادل بین المللی این استاندارد ,استاندارد (SDH) است .

در استاندارد SONET میزان پایه ای برای انتقال داده ها تعیین می شود و برای مقادیر بیشتر از آن از مضارب این میزان پایه استفاده می شود.میزان پایه را حامل نوری یا OC(Optical Carrier) می گویند.جدول زیر این مضارب را برای شما نمایش می دهد.

حامل نوری	میزان تبادل داده ها
OC-1	51.84 Mbps
OC-3	155.52 Mbps
OC-12	622.08 Mbps
OC-48	2.488 Gbps
OC-192	9.953 Gbps

ارتباط فیبر نوری (FDDI) :

این تکنولوژی از فیبر نوری به عنوان رسانه جهت انتقال داده ها استفاده می نماید.در این ساختار از یک حلقه برای انتقال داده ها و جلوگیری از بروز خطا در زمان انتقال استفاده می گردد. این ساختار در واقع ترکیبی از سرعت انتقال بالا در ساختار فیبر نوری و سیستم جلوگیری از خطا در ساختار "توکن رینگ" است.اولین بار این ساختار بر اساس استانداردی در سال ۱۹۸۶ بنا نهاده شد که بر مبنای آن امکان انتقال تکنولوژی عبور توکن ها بر روی بستر فیبر نوری با سرعت ۱۰۰ مگابیت در ثانیه فراهم می گردید.دامنه استفاده از این تکنولوژی به مرور کم تر شد تا امروزه به ندرت و آن هم در محل هایی با پهنای باند بالا استفاده می شود که قابل اطمینان بودن ارتباط از همه اصول دیگر در آنها مهم تر باشد.

پروتکل های ارتباط راه دور :

این پروتکل ها وظیفه مدیریت ارتباط راه دور را برعهده دارند.در این بخش با پروتکل های ارتباط راه دور که امروزه از آنها استفاده می شود آشنا می شویم:

- پروتکل (SLIP)

- ❖ پروتکل نقطه – به -نقطه (PPP) و نقطه – به -نقطه بر روی بستر اینترنت (PPoE)
- ❖ پروتکل تونل در ارتباط نقطه- به – نقطه (PPTP)
- ❖ سرویس دسترسی راه دور(RAS)
- ❖ سرویس صفحه کار راه دور (RDP)

پروتکل ارتباط سریال اینترنت(SLIP):

در سال ۱۹۸۴ دانشجویان دانشگاه برکلی این پروتکل را برای سیتم عامل لینوکس توسعه دادند.این پروتکل برای انتقال داده ها با کمک پروتکل TCP/IP بر روی ارتباط سریال بود.این ارتباط مانند ارتباط مودم با خطوط تلفن شهری بود.این پروتکل بر روی لایه های فیزیکی و پیوند داده ها عمل می نماید.امروزه این پروتکل در سیتم های عامل دیگری غیر از لینوکس هم کاربرد دارد. البته به مرور زمان نقش آن کم رنگ تر می شودو دلیلش عدم رقابت در امکانات در مقایسه با پروتکل های دیگر ارتباطی است.

> این پروتکل از رمز نگاری داده ها پشتیبانی نمی نماید . از این رو کلمات عبور و دیگر موارد حساس و امنیتی بصورت یک فایل متنی منتقل می شوند . با این شرایط براحتی می توان گفت که این پروتکل فاقد امنیت است.

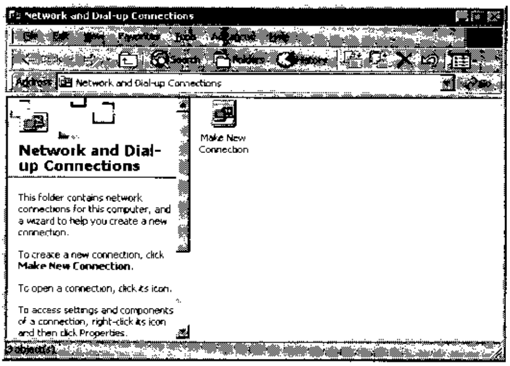
برقراری ارتباط با این پروتکل نیازمند یک حساب کاربری در سمت کاربر و اجرای یک اسکریپت بر روی ایستگاه کاری می باشد. که معمولا برقرای این نوع ارتباط راه دور بسیار مشکل است.پیشنهاد ما این است که حتی الامکان از این پروتکل استفاده نشود زیرا اکثر سیستم های عامل مانند ویندوز ۲۰۰۰ از ورود با این پروتکل به سیستم عامل پشتیبانی نمی نماید و تنها اجازه برقراری ارتباط از خود سیستم عامل با سیستم عامل لینوکس را صادر می نماید.

ارتباط نقطه – به -نقطه (PPP)و نقطه – به -نقطه بر روی بستر اینترنت (PPOE):

این پروتکل برار برقرای ارتباط بین دونقطه مانند ارتباط از طریق تلفن یا خطوط اجاره ای استفاده می شود.این اتصال بیشتر برای اتصال از راه دور به سرویس دهنده های اینترنت و اتصال راه دور به شبکه های محلی استفاده می شود.

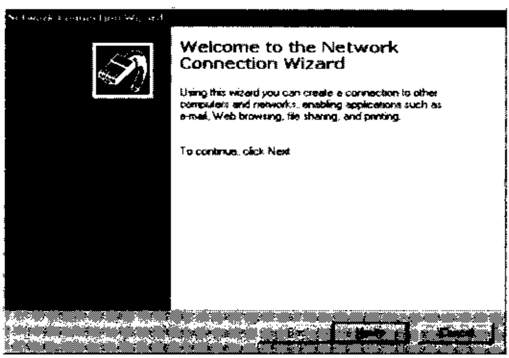
برای برقراری ارتباط و تبادل داه ها بین دو سیستم راه دور نقطه به نقطه از پروتکل کنترل کننده ارتباط یا LCP (Link Control Protocol) استفاده می شود.پروتکل LCP سلامت ارتباط را بررسی می نماید و پس از آن تنظیمات مر بوط به کاربران را تعیین می نماید.

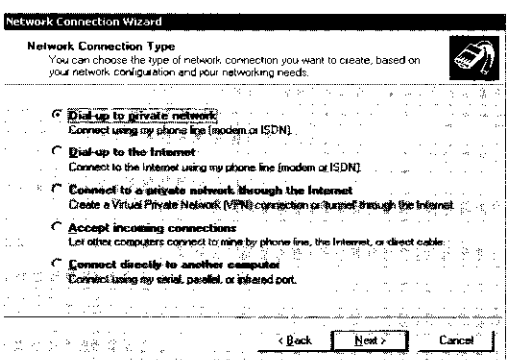
از نگاه فنی برای کارشناسان شبکه ، استفاده از پروتکل pppبسیار آسان است. پس از اولین اتصال به مسیریاب از طریق این پروتکل تمامی پارامتر های پروتکل TCP/IPتوسط مسیریاب تنظیم می گردد.تنظیمات مربوط به آدرس IPتوسط سرویس DHCPبصورت خودکار به کاربر اختصاص داده می شود.



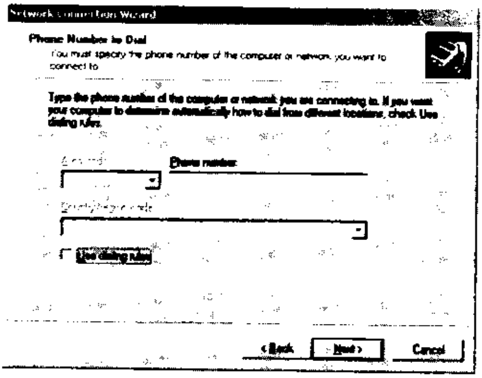
برای تنظیم هر رایانه با سیستم عامل ویندوز ۲۰۰۰ به منظور ارتباط راه دور با استفاده از پروتکل PPP این مراحل را می بایست ادامه دهیم.برای شروع کار ؛ از منوی شروع وارد کنترل پنل می شویم. سپس گزینه مربوط به شبکه را انتخاب می نماییم.

گزینه ساختن یک ارتباط جدید را انتخاب می نماییم.



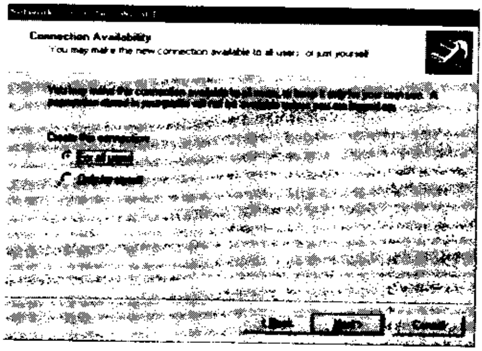


درقدم بعدی یکی از انواع ارتباطات را انتخاب می نماییم. در این حالت ما نیاز به برقراری ارتباط از طریق تلفن داریم.

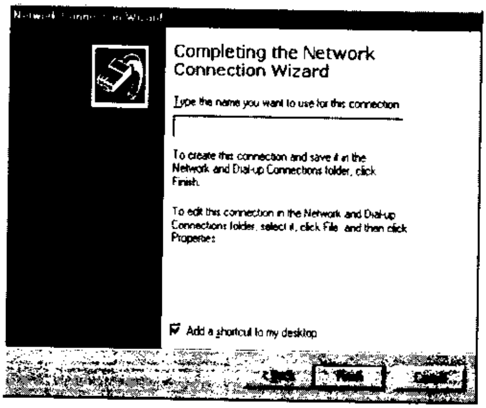


پس از انتخاب نوع ارتباط نوبت به ورود شماره جهت برقراری ارتباط خصوصی راه دور با پروتکل PPP می رسد.

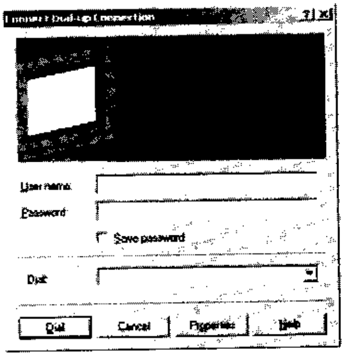
شما می توانید مشخص نمایید که این ارتباط قابل دسترس برای کدامیک از کاربران باشد. ارتباط می تواند قابل دسترس برای کاربر فعلی یا برای تمام کاربران باشد.



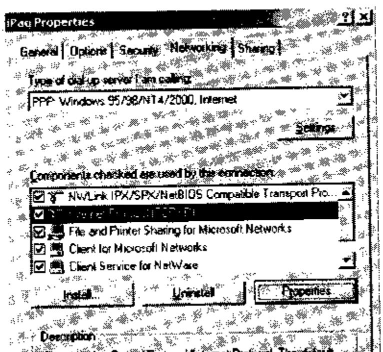
در این مرحله برای ارتباط یک نام انتخاب می نماییم. همچنین می توان انتخاب نمود که یک میانبر در روی کار نمایش قرار گیرد.



حال تمامی موارد ساخت یک اتصال جدید با موفقیت انجام شد.برای آغاز ارتباط می توان آن را از روی صفحه کار انتخاب نمایید. در این صفحه شما می توانید کلمه عبور و کد کاربری همچنین شماره تماس را وارد نمایید وارتباط را برقرار نمایید.



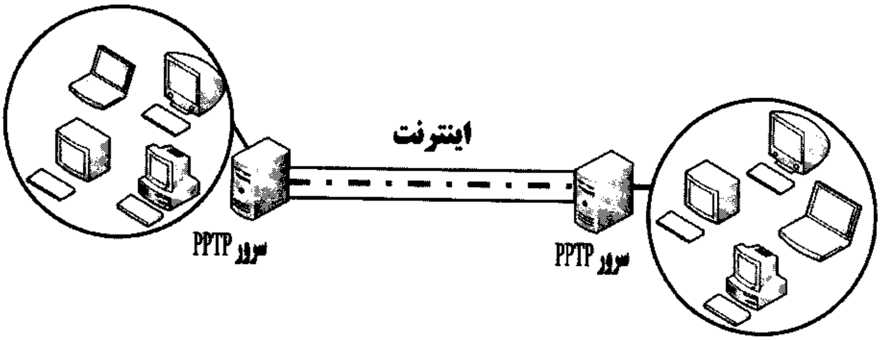
برای تغییر تنظیمات اتصال از منو تنظیمات استفاده می شود. تغییرات می تواند تغییر پروتکل یا آدرس IP باشد.همچنین امکان به اشتراک قرار دادن این اتصال برای کاربران شبکه هم می تواند فعال شود.



در این بخش تمامی موارد مورد نیاز برای برقراری یک ارتباط راه دور از طریق تلفن مورد بررسی قرار گرفت. ساختار دیگری از ارتباط PPP هم وجود دارد . PPPoE ارتباط PPP بر روی بستر اترنت است که اجازه بررسی اعتبار کاربران راه دور برروی بستر اترنت را فراهم می آورد.با این روش کاربران مستقل می توانند پس از بررسی اعتبار و تایید مجوز ورود ؛ از امکانات شبکه های پرسرعت اشتراکی مانند DSL استفاده نمایند.

ارتباط تونل نقطه – به –نقطه (PPTP) :

این پروتکل ساخته شرکت مایکروسافت است که بر مبنای پروتکل PPP طراحی شده است.در این ساختار یک اتصال مجازی بصورت یک تونل بین دو سیستم بر روی بستر اینترنت با پروتکل های TCP/IPو PPP برقرار می شود و داده ها از طریق این تونل بصورت کاملا امن به مقصد هدایت می شوند.



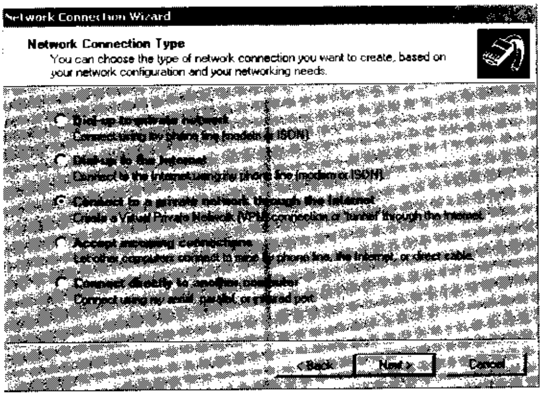
معمولا برای برقرای این ارتباط ابتدا یک ارتباط با کمک پروتکل PPP انجام می گیرد. سپس ارتباطی دیگر بر روی بستر ارتباط اولیه با کمک پروتکل PPTP برقرار می گردد.

داده ها بر روی تونل ایجاد شده بصورت کاملا خصوصی و امن بین مبدا و مقصد منتقل می شوند.این تونل تا زمان برقراری هرکدام از ارتباط ها بر قرار بوده و در صورت بروز اختلال در هرکدام از این ارتباطات تبادل داده ها از طریق این تونل امکانپذیر نخواهد بود.

هرگاه بستر ارتباط اولیه اینترنت باشد و تونل بر روی این بستر ایجاد شود ، شبکه ای ساخته می شود که به آن شبکه مجازی خصوصی یا VPN می گویند .این شبکه در مقایسه با راه اندازی یک شبکه اختصاصی و مستقیم بسیار ارزان تر بوده و ایجاد آن به راحتی امکانپذیر است .البته این روش معایبی هم دارد که برخی از آنها عبارتند از :

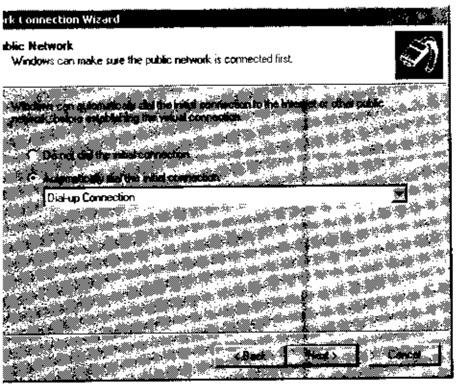
- بر روی همه سیستم ها قابل پیاده سازی نیست.
- برقراری آن در ارتباط با پروتکل PPP دشوار تر است.
- ایجاد تونل پهنای باند و میزان انتقال داده ها را کاهش می دهد.

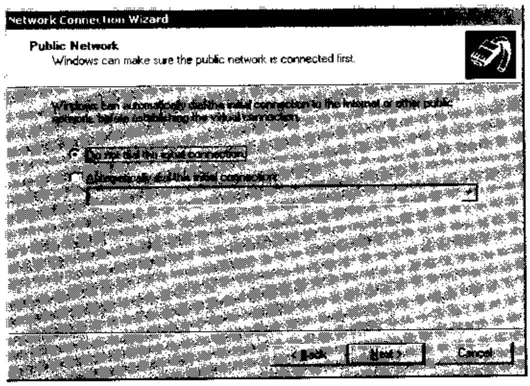
برای برقرای این ارتباط در ویندوز مراحل زیر را اجرا می نماییم : برای شروع کار ؛ از منوی شروع وارد کنترل پنل می شویم . سپس گزینه مربوط به شبکه را انتخاب می نماییم.

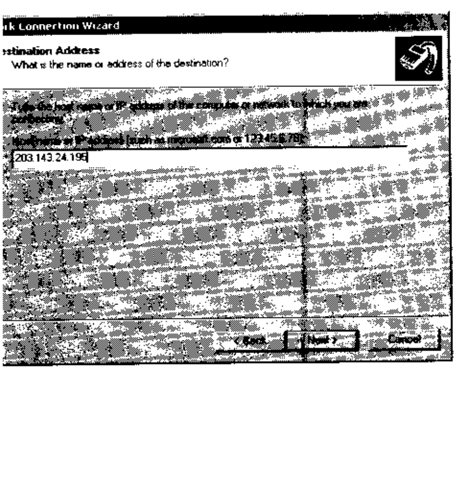


گزینه ساختن یک ارتباط جدید را انتخاب می نماییم.در این بخش برقراری ارتباط خصوصی را انتخاب می نماییم.

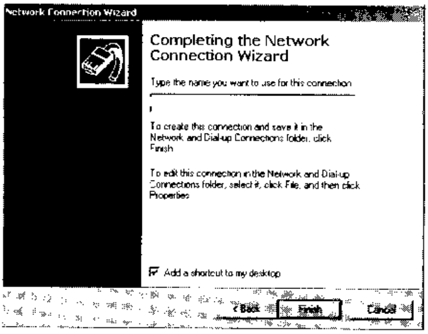
اگر سیستم هیچ ارتباطی به خارج نداشته باشد می بایست ابتدا به شبکه متصل شده و سپس یک تونل ایجاد نماید. در این بخش می توان مشخص نمود که نیاز به برقراری ارتباط اولیه می باشد یا خیر



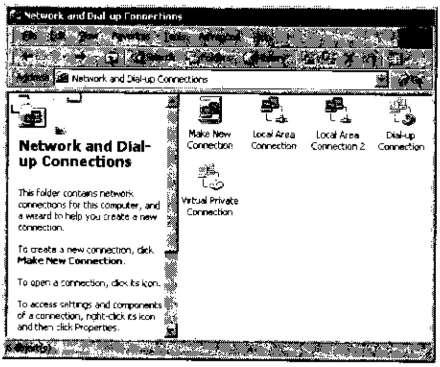




مرحله بعدی انتخاب سرور از طریق نام و یا آدرس IP آن می باشد.

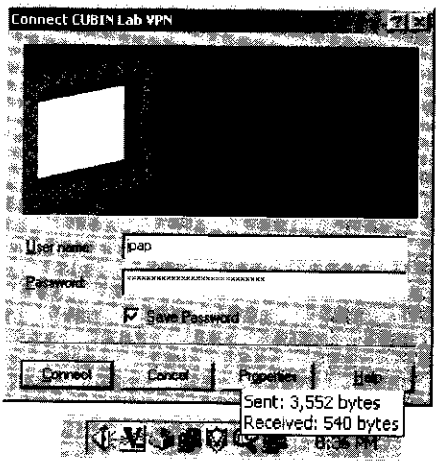


این مرحله انتخاب نام اتصال می باشد که آخرین مرحله ساخت اتصال می باشد.



برای تغییر تنظیمات همچنین برقراری یا قطع ارتباط می بایست به کنترل پنل وارد شده و سپس گزینه مربوط به شبکه را انتخاب نماییم.

برای برقراری ارتباط کد کاربری و کلمه عبور را وارد نموده و پس از تایید ارتباط برقرار می گردد.



سرویس دسترسی راه دور ویندوز (RAS):

نسخه های NT و ۲۰۰۰ ویندوز دارای قابلتی هستند که به کاربران اجازه می دهد که از راه دور به آنها متصل شده و نه تنها از امکانات سرور بلکه ازدیگر منابع شبکه هم استفاده نمایند. این امکان از طریق سرویس دسترسی راه دور ویندوز امکانپذیر می گردد . در این ساختار یک مودم و یک خط تلفن متصل به آن که می بایست به سرور متصل شده باشد فراهم کننده دسترسی است.

این سرویس در شبکه های بسیار کوچک که توانایی خرید تجهیزات مسیریابی و اتصال ندارند کاربرد دارد. از این رو استفاده از این سرویس بسیار محدود است.

سرویس صفحه کار راه دور (RDP) :

با استفاده از این سرویس کاربران می توانند به سیستم عامل ویندوز بصورت گرافیکی متصل شوند.دسترسی به سیستم با مجوز بوده و تنها کاربران مجاز امکان دسترسی را خواهند داشت.

این نوع ارتباط محدودیت هایی هم دارد که می توان به برخی از آنها اشاره کرد:

- تنها محدود به کاربران سیستم عامل ویندوز می باشد.
- امکان دریافت و ارسال فایل در این ساختار وجود ندارد.
- ارتباط گرافیکی نیازمند پهنای باند بالایی است.

از این ارتباط می توان برای رفع مشکلات سیستم از راه دور، پشتیبانی نرم افزار های کاربردی و بروز رسانی نسخه های نرم افزار های امنیتی استفاده نمود.

جمع بندی:

در این بخش شما:

- ❖ با تکنولوژی و ساختار ارتباطات راه دور آشنا شدید.
- ❖ انواع اتصال های راه دور شبکه و خصوصیات هرکدام را فراگرفتید.
- ❖ در مورد پروتکل های ارتباطی راه دور مطالب مهمی آموختید.
- ❖ با شبکه های خصوصی مجازی آشنا شدید.

سوالات ارزیابی برای آزمون Network+ :

۱ -کدام گزینه معایب پروتکل RDP یا صفحه ارتباطی راه دور را بیان می کند.(تمامی موارد صحیح را مشخص نمایید)

الف) محدود به کاربران سیستم عامل ویندوز است

ب) امکان دریافت و ارسال فایل وجود ندارد.

ج) ارتباط گرافیکی نیاز به پهنای باند بالا دارد.

د) سرعت اتصال همیشه پایین است.

۲-کدامیک از این پروتکل ها از رمز نگاری داده های انتقالی پشتیبانی نمی نمایند.

الف) SLIP

ب) RDP

ج) PPP

د) PPTP

۳-درگاهUSB از اتصال چند دستگاه بصورت همزمان پشتیبانی می نماید.

الف)۱۱۰

ب) ۴

ج) ۱۲۷

د) ۱۲۸

۴- کدام آدرس ها به ترتیب مربوط به IRQ و آدرس I/O درگاه Com4 می باشد.

الف) ۴ - 3F8

ب) ۳ - 2F8

ج) ۴ - 3F8

د) ۳ - 2F8

۵-کدام گزینه خصوصیات پروتکل PPP را بیان نمی نماید. (تمامی موارد صحیح را مشخص نمایید)

الف) امکان دریافت آدرس از DHCP را دارد.

ب) این ارتباط بر روی بستر اینترنت بر قرار می شود.

ج) این پروتکل از رمز نگاری داده ها پشتیبانی می نماند.

د) این ارتباط می تواند بصورت مستقیم بین دو سیستم بر قرار شود.

۶- برای برقرای ارتباط راه دور کدامیک از این تجهیزات ضروری است .(تمامی موارد صحیح را مشخص نمایید)

الف) صفحه کلید

ب) مودم

ج) نمایشگر

د) چاپگر

۷- کدام ساختار را نمی توان از خطوط دیجیتال دانست . (تمامی موارد صحیح را مشخص نمایید)

الف) T1.

ب) ISDN

ج) ADSL

د) Dial Up

۸-کدامیک از این موارد از مزایای استفاده از خطوط تلفن شهری است . (تمامی موارد صحیح را مشخص نمایید)

الف) در همه جا ی شهر موجود است.

ب) پهنای باند این خطوط از شبکه های محلی بالا تر است.

ج) هزینه استفاده از این خطوط برای انتقال داده ها ارزان است.

د) این خطوط بسیار قابل اطمینان بوده و هیچگاه در آنها اختلال مشاهده نمی شود.

۹- یک مودم داخلی از کدام درگاه برای اتصال به سیستم استفاده می نماید. (تمامی موارد صحیح را مشخص نمایید)

الف) درگاه سریال

ب) درگاه USB

ج) درگاه COM.

د) درگاه شبکه.

۱۰-کدامیک از این پروتکل ها برای ایجاد یک تونل بر روی بستر اینترنت استفاده می شود .

الف) HTTPS

ب) PPP

ج) PPTP

د) TCP

پاسخ به سوالات این بخش

۱ - **الف ،ب ،ج**

سرعت اتصال هیچگاه پارامتری از پیش تعیین شده نیست و به ساختار ارتباطی بستگی دارد.

۲ - **الف**

با توجه به توضیحات این فصل مشخص است که گزینه صحیح الف است..

۳ - **ج**

با توجه به توضیحات این فصل پاسخ صحیح مشخص است.تعداد این دستگاه ها می تواند حداکثر ۱۲۷ دستگاه برای هر درگاه باشد

۴ - **د**

با توجه به توضیحات این فصل گزینه صحیح د است.

۵ - **ب**

این ارتباط بین دو سیستم بر قرار می شود و نیازی به اینترنت برای برقراری این ارتباط وجود ندارد.

۶ - **ب**

مودم از ملزومات برقراری ارتباط راه دور و موارد دیگر از ملزومات و تجهیزات یک رایانه هستند .

۷ - **د**

همه موارد بجز Dial Up از ساختار های انتقال دیجیتال هستند..

۸ - **الف ،ج**

ارزان بودن و در دسترس بودن در همه نقاط شهر مزایای این ساختار می باشد.

۹ - **ج**

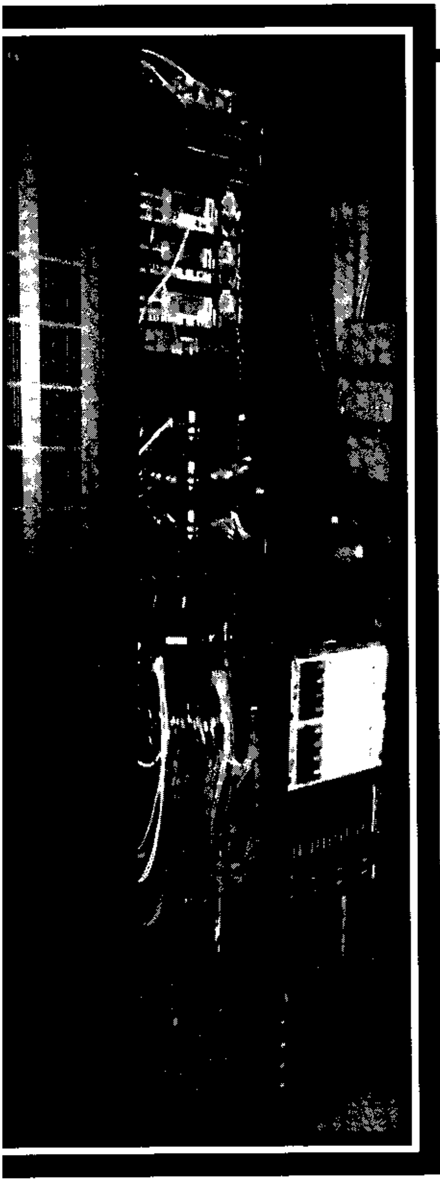
درگاه Com مربوط به مودم داخلی است و درگاه های دیگر می تواند در مودم های خارجی استفاده شود.

۱۰ - **ج**

Ppp برای ارتباطی دو سویه وPPTP برای ایجاد تونل بر روی بستر ارتباط دو سویه استفاده می شود.

فصل هشتم

دسترسی به شبکه و امنیت



شما در این فصل با این مفاهیم آشنا خواهید شد:

۸-۱ آشنایی با پروتکل های امنیتی و شناسایی عملکرد های هرکدام :

- IPSec
- L2TP
- SSL
- WEP
- WPA
- 802.1x

۸-۲ آشنایی با پروتکل های تصدیق اعتبار

- CHAP
- MS-CHAP
- PAP
- RADIUS
- KERBEROS
- EAP

۸-۳ مشخص نمودن عملکرد و دلایل استفاده از دیواره آتش

۸-۴ مشخص نمودن عملکرد و دلایل استفاده از دیواره سرویس پروکسی

8-۵ آشنایی با سیاست های امنیتی در شبکه

فصل هشتم- دسترسی به شبکه و امنیت

مقدمه:

برای سخن گفتن از امنیت هرگاه بخواهیم در مورد دسترسی به منابع در شبکه صحبت نماییم دو شرط لازم وجود دارد : دسترسی به شبکه و امنیت مناسب. با همکاری بین این دو بخش شما می توانید به منابع شبکه دسترسی پیدا نموده و از آنها استفاده نماید.

بخش اول تامین کننده دسترسی از سوی کاربران به شبکه است. برای این کار برخی از سیستم عامل ها نیاز به افزودن نرم افزار هایی دارند که بتواند دسترسی را ایجاد نماید.

شما به عنوان مدیر شبکه می توانید تدابیر امنیتی مورد نظر خود را طراحی و بر روی شبکه اجرا نمایید.در این فصل بحث ما بیشتر بر روی امنیت در شبکه و دسترسی به منابع شبکه است.همچنین در مورد تهدیدات شبکه و ابزار امنیتی برای جلوگیری از نفوذ به شبکه هم به اختصار می پردازیم.

> یکی از مواردی که در این بخش در مورد آن صحبتی نمی شود امنیت فیزیکی است. زیرا در سرفصل های آزمون +Network قرار ندارد.باید دقت نمایید که اگر کسی بتواند به اتاق سرور شما وارد شود و کنترل سرور های شما را در اختیار بگیرد عملا پروتکل های امنیتی هیچ کاربردی نخواهند داشت. شما باید همزمان با امنیت شبکه به امنیت فیزیکی شبکه هم بپردازید.

مدیریت کاربران و امنیت کلمات عبور

نام کاربری و کلمه عبور کلید ورود به مبحث امنیت شبکه است که از آن برای کنترل ورود به سیستم استفاده می شود.نام کاربری و کلمه عبور توسط مدیر شبکه تعریف شده و در اختیار کاربر قرار می گیرد . در برخی موارد به کاربر اجازه می دهند که کاربر بتواند کلمه عبور خود را تغییر دهد. در این صورت مسوولیت مدیر شبکه سنگین تر می شود. مدیر می بایست نحوه انتخاب یک کلمه عبور مناسب را به کاربران شبکه آموزش دهد. در این خصوص ما در این فصل سخن خواهیم گفت.

منابع شبکه و مدل های امنیت اشتراک قرار دادن منابع

شما در شبکه منابع بسیاری را مشاهده می نمایید که برای استفاده دیگر کاربران به اشتراک قرار داده شده است. این منابع به دو صورت به اشتراک قرار داده شده است:

- بر اساس سطح اشتراک
- بر اساس کاربر

اشتراک بر اساس کار بر مدیریت قوی تری را در اختیار مدیر شبکه قرار می دهد اما پیکر بندی اشتراک بر اساس سطح اشتراک بسیار آسانتر می باشد.

سطح اشتراک

در این روش برای دسترسی به منابع اشتراکی شبکه کلمه عبور تعریف می شود.این کار بجای تعریف حق دسترسی برای کاربران است.این کلمه عبور در اختیار تمام کاربرانی قرار می گیرد که نیاز به دسترسی به این منابع دارند.تمام کاربرانی که از این کلمه عبور اطلاع دارند می توانند منابع اشتراکی در شبکه را مشاهده نموده و در آنها تغییرات ایجاد نمایند. پیگیری تغییرات ایجاد شده توسط مدیر شبکه بسیار مشکل و در برخی موارد غیر ممکن است. استفاده از این روش تنها برای شبکه ها بسیار کوچک کاربرد دارد که بتوان موارد اشتراکی را بررسی و پیگیری نمود. این روش از سطح امنیت کمتری برخور دار است.

این روش در ویندوز ۹۵؛ ۹۸؛ NT؛ ۲۰۰۰ و ۲۰۰۳ از این روش پشتیبانی می نماید.

سطح کاربران

در این روش استفاده از منابع اشتراکی تنها برای کاربر خاصی مجاز است که با کد کاربری و کلمه عبور تعریف شده به شبکه وارد شده است. در این روش تنها کاربرانی که دارای کلمه عبور و کد کاربری تعریف شده هستند می توانند از هر کدام از منابع اشتراکی استفاده ننمایند. این روش کنترل و امنیت بیشتری را ایجاد می نماید زیرا دسترسی بر اساس اطلاعات حساب کاربری کاربران است و کاربران کلمه عبور خود را در اختیار دیگران قرار نمی دهند (و یا صحیح تر آن است که نباید قرار دهند) از این رو براحتی می توان بررسی نمود که کدام کاربر به منابع خاصی دسترسی داشته است و چه عملی بر روی آن انجام داده است.

در ویندوز NT؛ ۲۰۰۰ و ۲۰۰۳ و سیستم عامل های ناول و یونیکس از این روش پشتیبانی می گردد.

مدیریت حساب کاربری

اولین و مهمترین نکته در مدیریت حساب های کاربری طبقه بندی کاربران و ایجاد سطح دسترسی برای هر گروه از این کاربران می باشد. به عنوان مثال ممکن است سیاست شبکه شما بر این باشد که تنها گروه خاصی از کاربران امکان استفاده از چاپگر را داشته باشند و یا استفاده از منابع اشتراکی هر بخش تنها برای کاربران همان

بخش مجاز باشد همچنین می توانید زمان مجاز برای استفاده از منابع اشتراکی برای کاربران را هم معین نمایید و یا مدت زمان مجاز برای هر کاربر(به عنوان مثال یک هفته) جهت استفاده از کاربر هم در اختیار شما قرار می گیرد. شاید یکی از وظایفی که زمان زیادی را از مدیر شبکه در اختیار می گیرد همین بحث باشد.

غیر فعال کردن کاربران

زمانی که یک کاربر شبکه شما را ترک می نماید، شما می توانیدیکی از این ۳ کار را در مورد حساب کاربری او انجام دهید:

- حساب کاربری را به همان صورت رها نمایید.
- حساب کاربری را حذف نمایید
- حساب کاربری را غیر فعال نمایید.

اگر شما بخواهید حساب کاربری را به همان صورت رها نمایید هر کاربر که این نام کاربری و کلمه عبور را بداند می تواند وارد شبکه شود و یا حتی کاربری که شبکه شما را هم ترک کرده می تواند به شبکه وارد شود این کار امنیت شبکه شما را تهدید می نماید. حذف حساب کاربری هم مشکلات خاص خود را دارد.در صورت حذف این حساب تمامی دسترسی هایی اشتراکی که برای آن حساب تعریف شده بود هم حذف می شود. در صورتیکه کاربر برای مدتی شبکه شما را ترک کرده و احتمال دارد که به شبکه شما بازگردد به جای حذف می توانید آن را بصورت موقت غیر فعال نمایید تا در صورت بازگشت تنها نیاز به فعال سازی داشته باشد. و در صورتیکه بصورت دایم شبکه شما را ترک کرده است می توانید این حساب کاربری را تغییر نام داده و در اختیار کاربری جدیدی که جایگزین کاربر قبلی شده قرار دهیم. اما باید دقت نمود که تمامی دسترسی ها به حالت قبل باقی می ماند و در اختیار حساب کاربری با نام جدید قرار می گیرد.

غیر فعال کردن کاربران موقت

با افزایش قرارداد های موقت همه شبکه ها کاربرانی دارند که برای اجرای یک قرارداد در شبکه شما حاضر هستند و پس از اتمام قرار داد ، شبکه شما را ترک می نمایند.شما باید نحوه برخورد با این ورود و خروج این کاربران را مشخص نمایید. در بسیاری از شبکه ها به جای حذف این حساب ها تنها آنها را غیر فعال می نمایند تا در صورت بازگشت کاربر نیاز به تعریف مجدد حساب و دسترسی ها نباشد زیرا با حساب های غیر فعال شده نمی توان به شبکه وارد شد.

کاربران ناشناس

در بسیاری از شبکه ها برای دسترسی کاربران عادی به منابع شبکه امکان ورود به شبکه را با یک حساب کاربری یکسان فراهم می آورند.این کاربران می توانند از منابع شبکه بدون به جای گذاشتن هرگونه رد پایی استفاده نمایند. این کار می تواند امنیت شبکه را به خطر بیندازد. البته اگر شما به این کاربران تنها اجازه دسترسی محدود و آن هم به برخی منابع خاص را بدهید امنیت شبکه را به مخاطره نمی اندازد. و برای استفاده عمومی کاربران شبکه از این ساختار استفاده می شود.

محدود کردن اتصال ها

شما می توانید تعداد دفعاتی که یک کاربر می تواند به شبکه وارد شود را محدود نمایید.در این صورت تنها یک کاربر با نام کاربری می تواند به شبکه وارد شود. این کار می تواند از استفاده چند کاربر با نام کاربری یکسان بصورت همزمان جلوگیری نماید.این مورد در جایی کاربرد دارد که به دلیل اعمال برخی محدودیت ها کاربران بخواهند با استفاده از نام کاربری یک کاربر که محدودیت کمتری دارد از شبکه استفاده نماید.

همچنین می توان محلی که کاربر می تواند از آن به شبکه متصل شود را هم محدود نموده و از یک محل خاص به کاربر اجازه ورود به شبکه را داد. این کار می تواند دو جنبه داشته باشد یکی این که برخی سیاست های امنیتی بر روی سیستم عامل اعمال می شود و مربوط به یک رایانه می شود. با محدود کردن محل اتصال کاربر می توان این سیاست های امنیتی را هم به کاربر نسبت داد.

نام حساب های کاربری

در هر سیستم عامل نام هایی از پیش تعیین شده وجود دارد که با توجه به ماهیت حساب کاربری به آن اختصاص داده می شود.تقریبا اکثر این نام ها بین سیستم عامل های مختلف یکسان است.به عنوان مثال نام کاربری مدیر شبکه می تواند Administrator باشد. توصیه می شود که از آنها استفاده نمود.شما با توجه به ساختار شبکه نام های دیگری انتخاب نمایید تا نمایانگر هویت فردی کاربر باشد مثلا نام hamid بسیار مناسب تر از نام هایی مانند Admin یا Root می باشد. برخی از این نام ها که نباید مورد استفاده قرار گیرد عبارتند از :

- Admin
- Analyst
- Root
- Super User
- Manager
- Administrator
- Controller
- Super
- Supervisor
- Wizard

مدیریت کلمات عبور

همانند دیگر اجزای امنیت شبکه،کلمات عبور هم باید مدیریت شوند.این مدیریت مواردی را شامل می شود که باید رعایت شود تا بتواند کلمه عبور را تقویت نموده و امکان حدس زدن آن برای نفوذ گران تا حد ممکن دشوار باشد. و از این طریق مانع نفوذ و یا ورود بدون مجوز به شبکه شویم.

چگونه کلمه عبور را قدرتمند سازیم؟

بصورت عمومی ما کلمه عبوری را قوی می دانیم که ترکیبی از اعداد ؛حروف و کاراکتر های خاص باشد . همچنین این ترکیب باید آسان باشد تا کاربر بتواند آن را به خاطر بسپارد و برای حدس زدن نفوذ گران دشوار باشد متاسفانه بسیاری از کاربران به این موارد دقت نمی نمایند و کلمات عبوری انتخاب می نمایند که هم برا ی به خاطر سپردن خود آسان است و هم به راحتی می توان آن را حدس زد. در این بخش در مورد مواردی که کلمه عبور را تقویت می نماید صحبت خواهیم نمود.

حداقل طول

کلمات عبور نباید کمتر از ۸ کاراکتر و بیشتر از ۱۵ کاراکتر هم نباشند تا بتوان آن را به خاطر سپرد. کلمات عبور کمتر از این حد می توانند به راحتی حدس زده شود پس باید از این حداقل پیروی نمایید.زیرا مثلا در صورت استفده از ۳ کاراکتر تنها تعداد محدودی ترکیب وجود دارد که می توان آن را بسیار ساده تر از حالت هایی با تعداد کاراکتر بیشتر حدس زد.

لیست کلمات ضعیف

در این بخش می خواهیم برخی کلمات را شما هیچگاه نباید به عنوان کلمه عبور از آنها استفاده نمایید را اشاره نماییم. نفوذ گران معمولا ابتدا از این کلمات و ترکیبات این کلمات شروع می نمایند.

- کلمه Password
- نام و یا نام خانوادگی کاربر
- شماره شناسنامه کاربر
- شغل کابر
- کلمه Server
- هر ترکیبی از کلمات بالا با هم
- هر ترکیبی از این کلمات با کلماتی که دارای معنی هستند
- نام فرزندان کاربر
- محل تولد و سال تولد کاربر یا فرزندانش
- نام شرکت یا سازمان
- هر متنی که برروی رایانه یا نمایشگر نوشته شده
- کلمات مذهبی مانند نام پیامبران یا امامان
- هر ترکیبی از این کلمات با اعداد در ابتدا یا انتها
- هر ترکیبی از کلمات بالا که بصورت برعکس نوشته شده باشند

ممکن است ترکیبات دیگری هم وجود داشته باشد ما تنها به ذکر برخی از مهمترین موارد پرداختیم.

استفاده از کاراکتر های خاص برای تقویت کلمه عبور

کلمات عبور قوی حتما نباید برای به خاطر سپردن هم دشوار باشند.کاراکتر های خاص می توانند امنیت کلمه عبور را بهبود ببخشند.به عنوان مثال کلمه عبور tqb4f#hod6$ حاوی تمامی ترکیبات لازم برای یک کلمه عبور قوی است.

برای سنجش میزان قوت یک کلمه عبور از نرم افزار های خاصی که نفوذ به شبکه را شبیه سازی می نمایند استفاده می شود. شما خواهید دید حدس زدن کلمه عبوری که در آنها از کلمات عبور ترکیبی استفاده شده چقدر برای نرم افزار مشکل است و حدس آن زمان بسیار زیادی به طول خواهد انجامید. شما می توانید یک جمله را تقویت و آن را بصورت کلمه عبور استفاده نمایید. مانند under43gate@w#ay :

برخی دیگر از این ترکیب ها می توانند به این صورت باشد‌که شما می توانید خود این ترکیبات را ایجاد نموده و از آن استفاده نمایید:

- Run4!cov$er
- four@4for&
- Iron$steel%5
- Floor!7steel$

ساختار مدیریت کلمات عبور

تقریبا تمام سیستم های عامل دارای ساختاری هستند که کلمات عبور را مدیریت نموده تا سیستم همیشه امن باشد و مانع از نفوذ به شبکه شوند. این ساختار شامل :

- غیر فعال کردن خودکار حساب های کاربری
- تعیین تاریخ مصرف برای کلمه عبور

غیر فعال کردن خودکار حساب های کاربری

نفوذگران با مکانیزمی شبیه کاربرانی که کلمه عبور خود را فراموش کرده اند اقدام به حدس زدن کلمات احتمالی می نمایند. برای این که امکان نفوذ به شبکه با حدس زدن و ورود کلمات عبور را از بین ببریم ، سیستم های عامل امکانی دارند که با کمک آن در صورت تشخیص ورود چندین کلمه عبور نا درست حساب کاربری غیر فعال شود.در این صورت کاربر با ورود کلمه عبور صحیح هم نمی تواند به شبکه وارد شود و برای رفع این مشکل باید با مدیر شبکه تماس بگیرید تا حساب کاربری او فعال شود.

در شبکه هایی با امنیت بالا توصیه می شود که فعال سازی کاربران توسط مدیر شبکه انجام شود و بررسی دقیقی در مورد این اتفاق انجام شود که آیا کاربر کلمه عبور را فراموش نموده یا فرد دیگری به دنبال نفوذ به سیستم بوده است.

در بسیاری از سیستم های عامل تغییر کلمه عبور و یا فعال سازی حساب کاربری تنها می تواند توسط حساب کاربری با دستر سی مدیر سیستم انجام می شود. اگر رایانه ای تنها یک حساب مدیر دارد در صورت غیر فعال شدن این حساب نمی توان کاری برای فعال سازی آن حساب انجام داد.

تعیین تاریخ مصرف برای کلمه عبور

کلمه عبور حتی اگر در بهترین ساختار و قویترین امنیت باشد یک عمر دارد زیرا اگر بسیار طولانی از آن استفاده شود بالاخره توسط نفوذ گران کشف و مورد سوء استفاده قرار می گیرد. برای جلوگیری از این اتفاق برای کلمات عبور یک عمر مفید تعیین می شود و پس از آن کلمه عبور حذف شده و کاربر می بایست با کلمه عبور جدید به سیستم وارد شود و این چرخه در طول زمان تکرار می شود. در برخی شبکه ها این عمر ۳۰ روز است یعنی کاربر هر ماه باید کلمه عبور خود را تغییر دهد.این کار می تواند امنیت شبکه را افزایش داده و احتمال حدس زدن کلمات عبور را کاهش دهد.

کلمه عبور منحصر بفرد و تاریخچه کلمه عبور

در برخی نسخه های قدیمی تر سیستم های عامل ؛ پس از سر آمدن عمر مفید کلمه عبور ؛کاربر می توانست مجدد همان کلمه عبور قبلی را برای مدت مثلا ۳۰ روز استفاده نماید. به عبارت دیگر هیچ تغییری در کلمه عبور حاصل نمی شد. این کار با ماهیت تعیین عمر مفید برای کلمه عبور در تضاد بود زیرا کلمه عبور تغییر نمود. برای رفع این اشکال مهم تدبیری اندیشیده شد. کلمات عبور قبلی در سیستم ذخیره می شد. درصورتیکه کاربر همان کلمه عبور را وارد می کرد سیستم آن را نمی پذیرفت و از او درخواست می کرد که کلمه عبور جدیدی را وارد

نماید. این سیستم توانایی داشت تا تمامی کلمات عبور یک بازه زمانی را هم ذخیره نموده و در صورت تکرار هر کدام به کاربر اخطار داده و آن را هم نپذیرد.

بسیاری از کاربران عادت دارند که از یک کلمه عبور برای تمامی امور امنیتی خود استفاده می نمایند برای این کار یک کلمه عبور قوی تعیین می نمایند و آن را برای سیستم؛سرور ؛ کارت اعتباری و .... استفاده می نماید. با ایجاد این ساختار کاربر باید در طول هر بازه کلمه عبور مربوط به همه این موارد را تغییر دهد که کمی برای کاربر ایجاد مشکل می نماید.

سیستم های عامل جدید امکان ذخیره ۲۰ کلمه عبور را دارند که با توجه به ساختار امنیتی می تواند کلمات عبور مربوط به مدتی طولانی باشد.

استفاده از دیواره آتش

امروزه استفاده از اینترنت بسیار معمول است و تقریبا همه شرکت ها شبکه خود را به اینترنت متصل می نمایند. به بیان دیگر شبکه خصوصی خود را به یک شبکه عمومی متصل می نمایند. خصوصی از این بابت است که تنها کاربرانی می توانند از شبکه استفاده نمایند که عضو شبکه باشند و مجوز استفاده داشته باشند. برای محافظت از شبکه خصوصی در مقابل کاربران شبکه عمومی از دستگاهی ویژه با نام دیواره آتش استفاده می شود.

دیواره آتش در واقع ترکیبی از سخت افزار و نرم افزاری است که برای برای ماموریتی خاص پیکربندی شده اند. این ترکیب می تواند یک رایانه معمولی و یک نرم افزار و یا یک سخت افزار ویژه و یک سیستم عامل باشد. وظیفه اصلی بر عهده نرم افزار است که سیاست های امنیتی تعریف شده را بر روی سیستم پیاده می نماید. می تواند مانع دسترسی کاربران به برخی منابع در اینترنت شده و یا برخی محدودیت ها را برای کاربر در نظر بگیرد.

> شاید بسیاری از کارشناسان شبکه به منابعی برای نصب و پیکر بندی دیواره آتش دسترسی ندارند. در فصل ما نمی توانیم موارد امنیتی را پوشش دهیم زیرا این موارد می تواند خود مباحثی برابر با همین کتاب باشد اما سعی می نماییم برخی مفاهیم را بازگو نماییم که شما بتوانید با کمی مطالعه براحتی طرح امنیتی شبکه خود را مشخص و اجرا نمایید.

برخی از دیواره های آتش که به جعبه سیاه یا Black Box معروف هستند کاملا مجزا از سیستم عامل بوده و به تنهایی فعالیت می نمایند و از پایداری بالاتری برخور دار هستند زیرا سخت افزار و نرم افزار های آن فقط برای این کار طراحی و بهینه سازی شده اند و از این رو کارایی و توان اجرایی بالاتری دارند.

دیواره های آتش تنها بر روی نسخه های سرور سیسم عامل نصب می شوند نمی توان آنها را برروی سیستم های کاربری نصب نمود. امروزه برخی نرم افزار ها هستند که بر روی اکثر رایانه ها نصب می شوند این نرم افزار ها نسخه های شخصی دیواره آتش است و با نرم افزار هایی که منظور ما در این بخش هستند تفاوت دارد زیرا از آنها نمی توان برای تقویت امنیت شبکه استفاده نمود و تنها برای یک رایانه قابل استفاده است.

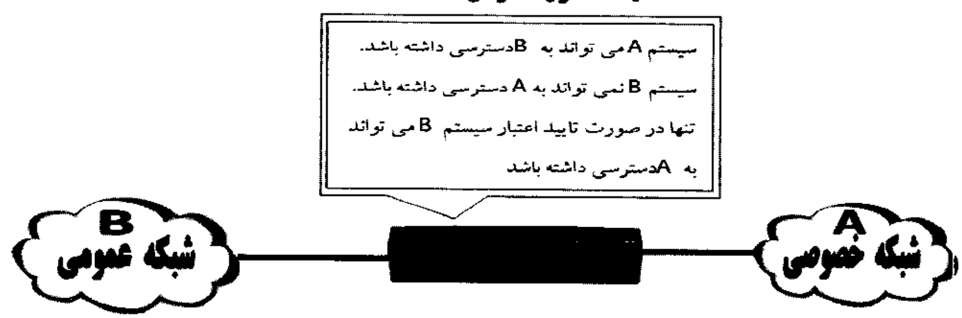
تکنولوژی های دیواره آتش

در دیواره های آتش از تکنولوژی های متفاوتی استفاده می شود که تفاوت آنها در نحوه محدود کردن ورود داده ها می باشد.برخی از آنها مانند کنترل دسترسی و کنترل داده های ورودی می تواند به عنوان دیواره های آتش استفاده شود که در برخی تجهیزات دیگر مانند مسیریاب ها از این ساختار ها برای افزایش امنیت استفاده می شود.

لیست کنترل دسترسی (Access Control List)

خط مقدم دفاع در مقابل حملاتی که از سوی اینترنت به شبکه خصوصی انجام می شود مشخص نمودن لیست دسترسی وکنترل دسترسی ها می باشد. این لیست مشخص می نماید که کدام آدرس IP مجوز ورود به شبکه و یا خروج از آن را دارد.این لیست می تواند بر روی مسیر یاب هم ذخیره شود و مسوولیت کنترل دسترسی بر عهده مسیر یاب باشد. زیرا مسیریاب به عنوان درگاه خروجی سیستم عمل می نماید.

لیست کنترل دسترسی



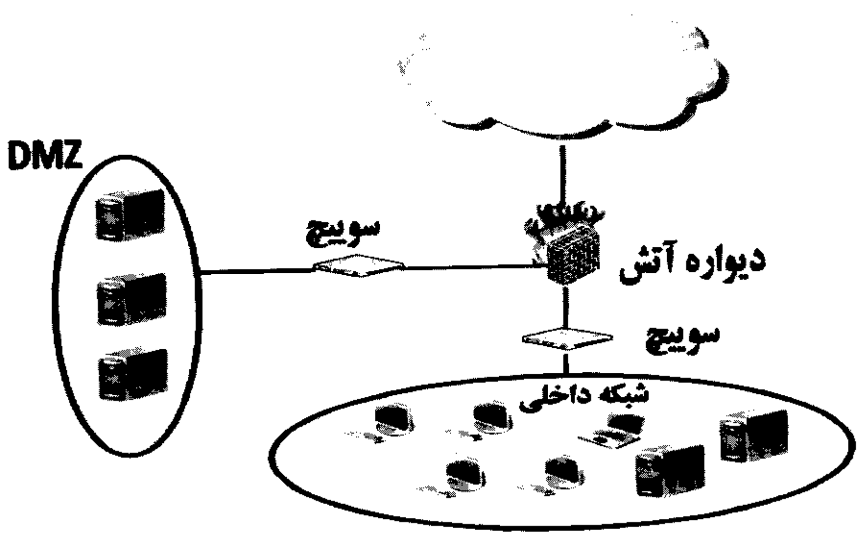
به عنوان مثال دسترسی از سمت شبکه خصوصی به عمومی مجاز است اما دسترسی از شبکه عمومی به خصوصی تنها با شرایط خاصی امکانپذیر است.برخی از نفوذگران داده های ورودی و خروجی شبکه را بررسی می نمایند به این کار Spoofing یا کلاهبرداری می گویند. در این روش نفوذگر داده هایی که کد گذاری نشده اند را به راحتی مشاهده می نماید. اگر کلمه عبور بصورت عادی منتقل شود آن را ذخیره و از آن برای نفوذ به شبکه استفاده می نماید. در این خصوص در ادامه این فصل بیشتر صحبت خواهیم کرد.

منطقه غیر نظامی DMZ(Demilitarized Zone)

اکثر دیواره های آتش امروزه از ساختاری استفاده می نمایند که به آن منطقه غیر نظامی یا DMZ می گویند. ساختار این ناحیه از شبکه، نه شبیه شبکه خصوصی است و نه عمومی بلکه دقیقا میان این دو ساختار است.

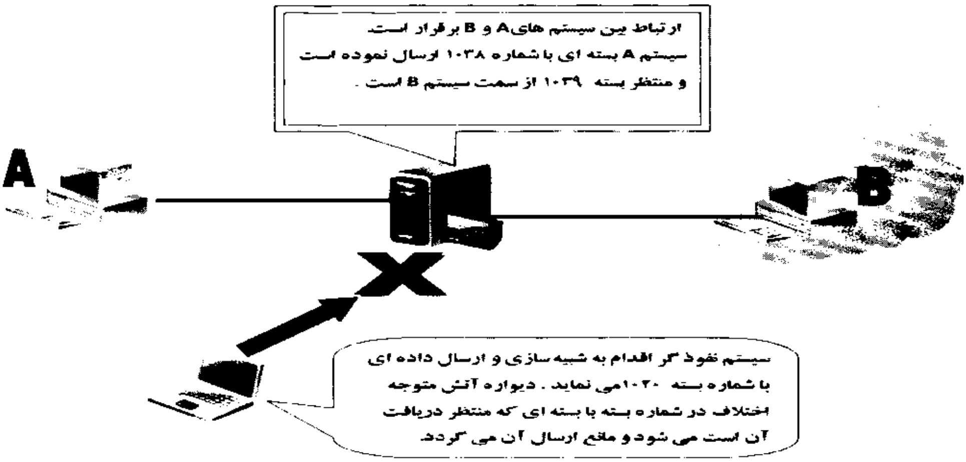
دیواره آتش در این ساختار دارای ۳ پورت شبکه است یکی برای اتصال به شبکه عمومی یا همان اینترنت، دیگری برای اتصال به شبکه خصوصی یا همان شبکه داخلی و سومی برای اتصال به DMZ استفاده می شود. اگر نفوذ گری به سرور ها وارد شود تنها داده های عمومی و شبکه عمومی را مشاهده می نماید و نمی تواند به داده های حساس و شبکه داخلی دسترسی داشته باشد زیرا این داده ها در بخش خصوصی شبکه نگهداری می شود.

در تصویر ساختار یک شبکه با یک دیواره آتش و ۳ ارتباط آن را مشاهده می نمایید.



پالایش داده ها

پالایش داده ها یا Packet Filtering در واقع مراحلی است که طی آن داده ها بررسی شده و در صورتیکه با قوانین تعریف شده امنیتی هماهنگ باشند اجازه عبور گرفته و در غیر اینصورت از ورود آنها به شبکه جلوگیری می شود. برای این منظور تمامی داده ها قبل از ارسال توسط دیواره آتش بررسی شده و آدرس های مربوط به گیرنده و فرستنده ثبت می گردد. این کار به این دلیل است که داده هایی که مربوط به یک جلسه تبادل داده هستند منتقل شوند و در صورت قطع جلسه و شروع جلسه جدید تمامی مراحل از ابتدا آغاز شود.این کار باعث می شود که نفوذ گران نتوانند با ارسال داده هایی شبیه داه های اصلی بتوانند به شبکه نفوذ نمایند.

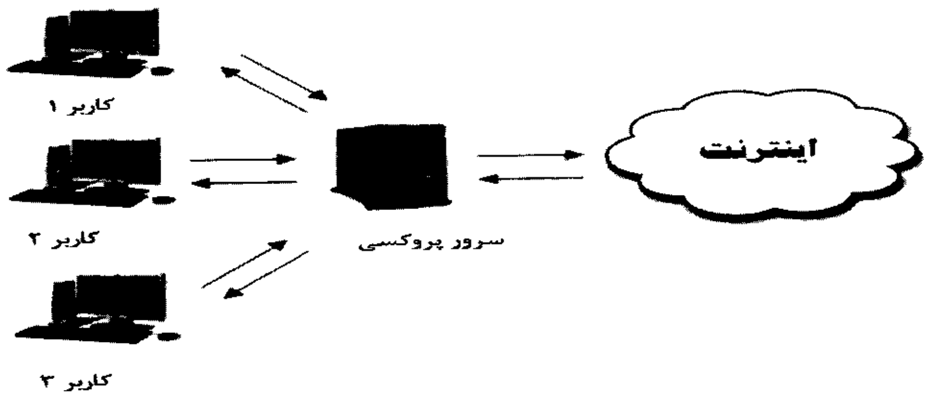


سرور پروکسی

سرور پروکسی یا به اختصار پروکسی ، به عنوان نماینده شبکه عمل می نماید و ارتباط بین شبکه داخلی و اینترنت را برقرار می نماید.فرض کنید یک سیستم قصد برقراری ارتباط با اینترنت را دارد بدون حضور پروکسی درخواست دریافت داده را ارسال نموده و داده مورد نظر را دریافت می کند. اما با حضور پروکسی درخواست خود را به پروکسی ارسال می نماید ،پروکسی هم به نمایندگی از آن سیستم درخواست را ارسال می نماید و داده مورد نظر را دریافت و برای سیستمی که درخواست کرده بود ارسال می نماید.

این کار باعث می شود که ارتباطی بصورت مستقیم بین سیستم های شبکه داخلی و اینترنت برقرار نشود و اگر کسی قصد نفوذ به شبکه کاربران را داشته باشد موفق به انجام این کار نگردد.

پروکسی ها معمولا دیواره های آتش بسیار قوی هستند زیرا محتوای تمام داده ها را بررسی نموده ودر صورت مشاهده هر داده مشکوک آن را حذف نموده تا به سیستم های کاربران صدمه ای وارد نشود همچنین می توانند داده ها را از نظر آلودگی به ویروس و نرم افزار های مخرب هم بررسی نموده و آلودگی احتمالی را تشخیص داده و مانع انتشار در شبکه گردد.



بطور کلی پروکسی ها را می توان به شاخه های زیر تقسیم نمود:

پروکسی IP

در این ساختار پروکسی آدرس تمامی سیستم های شبکه داخلی را هنگام درخواست داده از اینترنت با آدرس خود عوض می نماید و در ظاهر به نظر می رسد که داده ها مستقیم از سرور پروکسی ارسال شده و برای سرور دریافت می شود. این کار باعث می شود تا نفوذگران نتوانند از آدرس شبکه داخلی مطلع شده و مستقیم با آنها در ارتباط باشد.

پروکسی وب

این سرور درخواست های مربوط به پروتکل HTTP که همان پروتکل صفحات وب است را به عنوان نماینده کاربران ارسال می نماید و محتوای دریافتی را برای کاربر ارسال می نماید اگر این سرویس به درستی پیکر بندی شده باشد تمامی درخواست های کاربران در مرورگر اینترنتی مستقیم به سرور پروکسی ارسال می گردد و هیچ درخواستی بدون ارسال به پروکسی نمی تواند مستقیم به اینترنت ارسال شود.

یکی از موارد استفاده از این ساختار اضافه کردن یک Cache Server است. این سرور محتوای درخواستی کاربران را آرشیو و ذخیره می نماید. در صورتیکه در خواست یک کاربر در آرشیو موجود بود بدون اتصال به

اینترنت آن را برای کاربر ارسال می نماید اما در صورتیکه در آرشیو موجود نبود آن را از اینترنت دریافت می نماید، و پس از ذخیره آن را برای کاربر ارسال می نماید. نکته ای که باید به آن دقت نمود آن است که تنها داده های عمومی در آرشیو سرور ذخیره می گردد یعنی کلمه عبور کاربر برای ورود به سایت ها و پست الکترونیک هیچگاه در سرور ذخیره نمی گردد. با این روش امنیت شبکه بسیار بالا می رود زیرا تنها داده های مجاز وارد شبکه می شوند و از ورود داده های نامطمئن و خطرناک مانند اسکریپت های امنیتی به شبکه جلوگیری می نماید.

پروکسی FTP

این سرور ارسال و یا دریافت فایل از سرور را به نمایندگی از کاربران انجام می دهد.از نظر نحوه عملکر این سرور تقریبا شبیه پروکسی وب عمل می نماید

پروکسی پروتکل SMTP

این سرور تبادل پست الکترونیکی کاربران را بر عهده دارد. تمامی محتوای پست الکترونیک کاربران بصورت خود کار بررسی می گردد.هر داده ای که از نظر امنیتی مناسب تشخیص داده شود حذف شده و اجازه ارسال یا دریافت آن صادر نمی شود. این امکان با همکاری یک نرم افزار امنیتی که امکان بررسی آلودگی در برابر ویروس را دارد انجام می گیرد.

> شاید شما دیواره آتش سراغ داشته باشید که آن را نتوان در این تقسیم بندی ها قرار داد.برخی تولید کنندگان برای اینکه محصول خود را منحصر بفرد نمایند امکاناتی خاص به آن اضافه می نمایند که تقسیم بندی آن را مشکل و یا غیر ممکن می نماید.

پروتکل های امنیتی

امنیت داده هایی که بر روی اینترنت منتقل می شوند یکی از نگرانی های عموم کاربران شبکه اینترنت است. در اکثر مواقع داده ها بدون وجود هرگونه رمزنگاری بر روی بستر اینترنت منتقل می شوند.داده های حساس مانند حساب های بانکی ، کارت های اعتباری و پست الکترونیک در این روش بسیار آسیب پذیر هستند و امکان فاش شدن آنها زیاد است. برای رفع این مشکل از پروتکل های امنیتی استفده می شود . این پروتکل ها در واقع

مشخص کننده سیاست امنیتی است که چگونه داده های حساس بر روی شبکه منتقل شوند. تعداد این پروتکل های امنیتی زیاد است اما آزمون +Network تنها از شما آشنایی با این پروتکل ها را انتظار دارد.

- پروتکل تونل لایه دوم (L2TP)
- پروتکل امنیت اینترنت (IPSec)
- لایه ارتباط امن (SSL)
- کربروس (Kerberos)
- حریم خصوصی مانند ارتباط سیمی(WEP)
- ارتباط Wi-Fi محافظت شده (WPA)
- پروتکل تایید اعتبار کاربر (EAP)
- 802.1x
- پروتکل تصدیق اعتبار با کلمه عبور(PAP)
- پروتکل تصدیق اعتبار دو طرفه (CHAP)
- پروتکل تصدیق اعتبار دو طرفه برای سیستم عامل مایکروسافت (MS-CHAP)
- پروتکل تصدیق اعتبار راه دور (RADIUS)

پروتکل تونل لایه دوم

این پروتکل برای انتقال داده ها با پروتکل هایی غیر از TCP/IPبصورت خصوصی (VPN) بر روی بستر اینترنت طراحی شده بود. زیرا پروتکل مورد استفاده در اینترنت TCP/IP بوده و پروتکل های دیگر بدون تغییر نمی توانستند از این بستر عبور نمایند.در زمانی که دو شبکه پروتکلی غیر از TCP/IP داشته باشند و بخواهیم آنها را از بستر اینترنت به هم متصل نماییم این ساختار بهترین انتخاب می تواند باشد. این پروتکل در لایه دوم مدل OSI فعالیت می نماید.

پروتکل امنیت اینترنت

این پروتکل برای انجام تصدیق اعتبار کاربران و رمز نگاری داده ها بر روی شبکه اینترنت طراحی شده است.این پروتکل در لایه شبکه فعالیت می نماید و از آنجا که از هر دو نسخه ۴ و ۶ پروتکل IP پشتیبانی می نماید به سرعت به عنوان یک استاندارد برای شبکه های خصوصی یا VPN تبدیل شد.

ارتباط لایه امن(SSL)

SSL پروتکلی است که توسط شرکت Netscape طراحی شده بود که برای استفاده کاربران مرورگر اینترنت ساخته شده توسط این شرکت بود.این پروتکل امکان برقراری ارتباط بین سرور و کاربر را فراهم می آورد.از طریق این پروتکل بسیاری از نر افزار های کاربردی هم می توانند ارتباط امن برقرار نمایند. پروتکل HTTPS هم بر اساس این پروتکل بنا نهاده شده و می توان صفحات اینترنتی را بصورت امن مشاهده و داده ها را هم کاملا امن ارسال نمود. ارتباط کاربران بانک ها از طریق اینترنت می توانند عملیات بانکی را با امنیت کامل انجام دهند.

کربروس

کربروس در واقع یک پروتکل نیست بلکه سیستمی امن است. این ساختار توسط دانشگاه MIT طراحی شده بود.در این روش هویت هرکاربر زمانی که برای اولین باربه شبکه با کمک این پروتکل متصل می شود ثبت می شود و از آن برای تایید هویت در هر ارتباط مورد استفاده قرار می گیرد.در این پروتکل تمامی ارتباطات توسط رمز نگاری بسیار قوی انجام می شود. این پروتکل رایگان بوده و از اینترنت قابل دریافت می باشد.

حریم خصوصی مانند ارتباط سیمی (WEP)

این ساختار برای ایجاد یک امنیت حداقلی برای شبکه های بیسیم با استاندارد 802.11b مورد استفاده قرار می گیرد.با این پروتکل داده هایی که از این بستر منتقل می شوند رمزنگاری شده و بصورت امن منتقل می شود.داده ها توسط روشی خاص رمز نگاری می شوند که در صورت دسترسی یک نفوذگر به داده های منتقل شده دسترسی پیدا نماید این داه ها بصورت رمز بوده و نمی تواند از آنها استفاده نماید.

ارتباط Wi-Fi محافظت شده (WPA)

این ساختار امنیت شبکه های بیسیم را به نحو قابل ملاحظه ای ارتقا بخشید.این ساختار با ساختار WEP کاملا سازگار بوده ودر مورد تجهیزاتی که از آن پشتیبانی می نمودند تنها با یک بروز رسانی ساده قابل اجرا می باشد. برای اجرای این ساختار امنیتی پیشرفته دو روش وجود دارد ساختار TKIP و تایید کاربر .در ساختار TKIP(Temporal Key Integrity Protocol) داده ها بر اساس یک کلید رمز نگاری می شوند و کشف این رمز برای نفوذگران بسیار مشکل خواهد شد.

در ساختار تایید اعتبار کاربر؛ تنها کاربرانی که حساب کاربری مجاز داشته باشند امکان ورود به شبکه و استفاده از منابع آن را دارند و ورود برای افراد غیر مجاز امکانپذیر نیست.

پروتکل تایید اعتبار کاربر (EAP)

این پروتکل افزونه ای است که به پروتکل PPP اضافه می شود و امکان تایید اعتبار را برای کاربران راه دور فراهم می آورد.این پروتکل می تواند بر اساس نام کاربری و کلمه عبور صلاحیت کاربر را تایید نماید و یا این کار توسط اسکنر اثر انگشت ،تایید صدای کاربر و یا اسکنر قرنیه چشم هم باشد.

802.1x

زمانی که بنیاد بین المللی IEEE متوجه وجود رخنه های امنیتی در شبکه های بیسیم گردید برای حل این مشکلات امنیتی استانداردی را برای تایید اعتبار کاربران طراحی نمود.در این روش کاربر به نقطه دسترسی بیسیم متصل می تواند و کد کاربری و کلمه عبور خود را وارد می نماید. این اطلاعات به سروری که حساب های کاربری بر روی آن ذخیره شده است منتقل شده و در صورت تایید کاربر می تواند از منابع شبکه استفاده نماید. تا قبل از این مرحله کاربر علیرغم اتصال به شبکه از هیچیک از منابع شبکه نمی تواند استفاده نماید.با توجه که برای ورود به شبکه نیاز به تایید اعتبار وجود دارد این روش می تواند امنیت شبکه را ارتقا دهد.

پروتکل تایید اعتبار با کلمه عبور (PAP)

فارغ از متد های مختلفی که برای تایید اعتبار کاربران بکار می رود این روش را می توان ساده ترین روش دانست.در این روش اطلاعات حساب کاربری مانند نام کاربری و کلمه عبور بصورت نوشته عادی و بدون هیچگونه رمز نگاری بر بستر شبکه منتقل می شود.پس از رسیدن به سرور در صورتیکه باکد کاربری و کلمه عبوری که در سرور ثبت شده و مجاز است یکسان بود اعتبار کاربر تایید می شود.

علاوه بر ساده بودن در استفاده این روش ، امنیت آن بسیار شکننده است زیرا اطلاعات حساب های کاربری به راحتی قابل مشاهده برای نفوذگران است. هر فردی با در اختیار داشتن نرم افزار های خاصی با نام ابزار Sniffing می تواند به این اطلاعات که در شبکه منتقل می شوند دسترسی پیدا کند.

پروتکل تایید اعتبار دو طرفه (CHAP)

این پروتکل نسخه تکامل یافته پروتکل قبلی است. تفاوت عمده این دو پروتکل نحوه ارسال اطلاعات حساب کاربری می باشد. در این روش نام کاربری و کلمه عبور بر روی روی شبکه منتقل نمی شود.و به جای آن در هر

دو سمت کاربر و سرور با یک عبارت یکسان پیکربندی شده اند که به آن رمز اشتراکی یا Shared Secret می گویند. هرگاه کاربر درخواست تایید اعتبار نماید, سرور یک عبارت تصادفی با نام nonce به همراه یک شماره منحصر بفرد را برای کاربر ارسال می نماید.کاربر این دو عبارت را باهم ترکیب نموده و آن را با کمک الگوریتم رمزنگاری MD5 تبدیل به عبارتی نموده و آن را برای سرور ارسال می نماید. سرور این عبارتها را با هم مقایسه می نماید در صورتیکه عبارتها یکسان بود کاربر تایید و در غیر اینصورت کاربر غیر مجاز خواهد بود.

پروتکل تایید اعتبار دو طرفه برای سیستم عامل مایکروسافت (MS-CHAP)

شرکت مایکروسافت هم پروتکل های تایید اعتبار مخصوص به خود را دارد.این پروتکل از لحاظ عملکرد تقریبا شبیه پروتکل تایید اعتبار دو طرفه است اما در برخی موارد تفاوت هایی هم دارد.اولین تفاوت ، در پروتکل تایید اعتبار دو طرفه رمز اشتراکی بصورت یک عبارت بدون رمز نگاری در سیستم نگهداری می شود مایکروسافت تصمیم به رفع این مشکل گرفته و رمز اشتراکی را رمز نگاری می نماید.همچنین مایکرو سافت پروتکل رمز نگاری DES را بکار می گیردو این پروتکل تنها در سیستم عامل های خانواده ویندوز کاربرد دارد و در سیستم های عامل دیگر قابل استفاده نیست.

پروتکل تایید اعتبار راه دور(رادیوس)

این پروتکل برای تایید اعتبار کاربران از راه دور مورد استفاده قرار می گیرد.بیشتر در مراکز سرویس دهنده اینترنت برای بررسی اعتبار و میزان مصرف کاربران استفاده کننده از سرویس از این پروتکل بهره گرفته می شود. از این پروتکل فارغ از نوع ارتباط برای انواع ارتباطات می توان استفاده نمود.

این پروتکل در دیواره آتش هم مورد استفاده قرار می گیرد. هرگاه کاربر بخواهد از درگاهی خاص استفاده نماید باید با ورود کلمه عبور خود تایید اعتبار شود برای این کار اطلاعات کاربری به سرور رادیوس ارسال می شود تا پس از تایید امکان دسترسی به آن درگاه برایش فراهم گردد.

مقایسه سیستم عامل های دیواره آتش

بسیاری از دیواره های آتش بصورت ترکیبی از سخت افزار و نرم افزار مورد استفاده قرار می گیرد.سخت افزار دستگاهی از خانواده سرور ها می باشد و نرم افزار آن برای مقصد خاصی تهیه و بر روی یک سیستم عامل نصب شده است و از این سیستم تنها برای همین مقصود استفاده می شود یعنی برای اشتراک فایل یا چاپگر نباید مورد استفاده قرار گیرد زیرا این کار امنیت این سیستم را به خطر می اندازد.در این بخش ما به مروری اجمالی از سیستم عامل های شبکه و چگونگی پیکربندی دیواره آتش بر روی آن می پردازیم.

در کنار نرم افزار دیواره آتش ما نیاز به حداقل ۲ کارت شبکه برروی سیستم دارید. اگرچه بسیاری از این نرم افزار ها نیاز به ۳ کارت شبکه برای فعالیت دارند.

سیستم عامل یونیکس

یونیکس همانگونه که در مباحث قبل ذکر کردیم سیستم عاملی است که شبکه اینترنت بر آن بنا نهاده شده است. همچنین سیستمی است که دیواره آتش هم بر روی این سیستم عامل می تواند فعالیت نماید. یکی از محاسن این سیستم عامل آن است که شما می توانید برخی از سرویس های آن را فعال و برخی را غیر فعال نمایید.به بیان دیگر شما می توانید تمامی سرویس ها بجز دیواره آتش را غیر فعال نمایید و در این حالت سیستم یک دیواره آتش به تنهایی است. کارشناسان این سیستم را امن ترین سیستم عامل شبکه می دانند زیرا تنها سرویس های مورد نیاز و ضروری در سیستم فعال بوده و سرویس های دیگر می تواند غیر فعال و یا حذف گردد.اگرچه که مدیران خبره و کارآمد ویندوز و ناول هم می توانند همین کار را با آن سیستم عامل هم انجام دهند.

همانگونه که گفتیم دیواره آتش نیاز به تعدادی کارت شبکه برای فعالیت دارد. حداکثر تعداد کارت شبکه های مجاز در یونیکس ۳۲ ، در ناول ۱۶ و در ویندوز ۴ می باشد.همانگونه که قبلا هم ذکر کردیم این سیستم عامل بر اساس خط فرمان عمل نموده و در آن کمتر از گرافیک استفاده شده است از این رو سیستم عاملی کاربر پسند نمی باشد. اما پس از استفده از رابط های گرافیکی در این سیستم عامل دیواره های آتش مبتنی بر این سیستم عامل بیشتر مورد توجه کاربران قرار گرفته است.

نکته اساسی دیگر سرعت دیواره آتش است زیرا این سیستم باید هزاران و یا شاید میلون ها بسته داده را در هر ثانیه مورد بررسی قرار دهد.بسیاری از شرکت ها نرم افزار های خود را برای سیستم عامل های مختلف تهیه می کنند ،در مقایسه نرم افزار هایی که برای این سیستم عامل تهیه شدند بسیار سریعتر از دیگر سیستم عامل ها می باشد.

سیستم عامل ناول

اولین دیواره آتش که برای این سیستم عامل طراحی و اجرا شد مدیر مرزی یا Border Manager بود. این نرم افزار بر روی سیسم عامل نصب و تمامی تنظیمات از طریق سیستم عامل اجرا می شود. اما برخی موارد مانند سرعت و پشتیبانی از کاربران را می توان از محاسن این ساختار دانست و آن را یک دیواره آتش ایده آل برای مدیران با تجربه این سیستم عامل باشد .

از نگاه کارشناسان این سیستم عامل سریع ترین و به صرفه ترین دیواره آتش است اما از آنجا که کار با این سیستم عامل کمی مشکل است طرفداران کمی در بازار های تجاری دارد .

ویندوز

همانگونه که این سیستم عامل بسار پر طرفدار و همه گیر شده است شرکت های تولید کننده نرم افزار به فکر تولید دیواره آتش نرم افزار های بر پایه این سیستم عامل افتاده اند.به دلیل برخی مشکلات امنیتی در این سیستم عامل کمتر از آن برای دیواره آتش شبکه استفاده می شود.همزمان با رفع این مشکلات در نسخه های ۲۰۰۰ و بعد از آن استفاده از این سیستم عامل ها بیشتر استفاده می شود.

یکی از مهمترین محاسن دیواره های آتش ویندوزی مدیریت آنها از طریق رابط گرافیکی آنها است که کاملا شبیه عملکرد عمومی ویندوز است و تنظیم آن برای کاربر می تواند بسیار آسانتر باشد . اما در کنار این حسن سرعت ویندوز بالا نیست برای رفع این مشکل برخی کارت های افزودنی وجود دارد که می تواند توان اجرایی دیواره آتش را افزایش داده و آن را به سیستمی قوی تر تبدیل نمود.

جعبه سیاه

استفاده از این دستگاه می تواند یکی دیگر از انتخاب های شما باشد.شما بعد از خرید این دستگاه شما ممکن است اصلا ندانید که سیستم عاملی که در آن بکار رفته چیست. اما شاید به جرات بتوان گفت که هرچه باشد ویندوز نیست. معمولا سیستم عامل آن نسخه ای خاص از یونیکس است که برای فعالیت به عنوان دیواره آتش بهینه سازی شده است که در بین انتخاب های دیگر بالاترین توان اجرایی و سرعت را دارا می باشد. یکی دیگر از محاسن این دستگاه سهولت کاربرد آن است زیرا شما تنها برخی ساست های امنیتی مورد نظر خود را تغییر می دهید و نیاز به پیکر بندی اولیه و نصب سیستم عامل ندارند. شما یک بار تنظیمات مورد نظر خود را انجام می دهید و می توانید تا مدت ها از این دستگاه استفاده نمایید و خاطری جمع از امنیت شبکه خود مشغول مدیریت شبکه خود باشید .

یکی از مهمترین معایب این دستگاه این است که قابلیت ارتقا ندارد و پس از مدتی استفاده شما باید آن را با مدل هایی با کارآیی بالاتر تعویض نمایید.سیستم امنیتی ASA و PIX ساخت شرکت سیسکو یکی از معروف ترین نمونه های این ساختار است.

در سیستم های تجاری شما با برخی عناوین روبرو می شوید که شاید در هیچ کتابی در مورد آن صحبت نشده است. یکی از این مفاهیم UTM است. این دستگاه های ابزار های یکپارچه امنیتی هستند که علاوه بر دیواره آتش دارای ساختار شناسایی حملات ،شناسایی ویروس ها و بد افزار ها هم هستندکه می تواند تمامی خدمات امنیتی را بصورت یکپارچه در اختیار کاربر قرار دهند. امروزه استفاده از این تجهیزات بسیار متداول است.

مفهوم مقابله در مقابل حملات نفوذگران

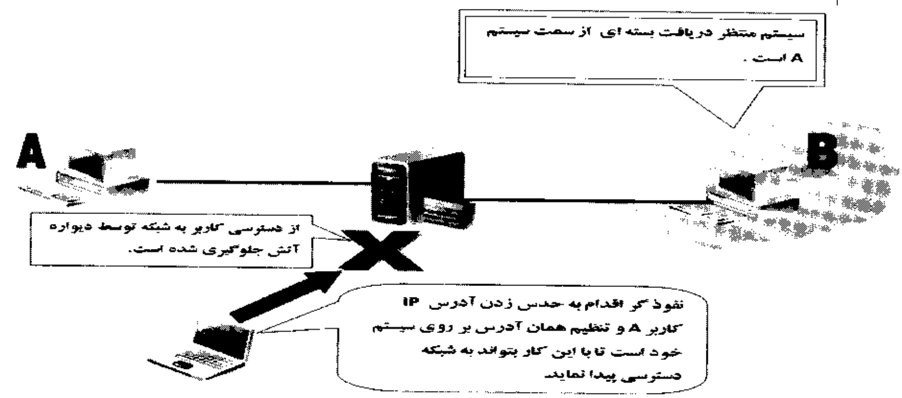
شما می توانید فعل و انفعالات صورت گرفته بین یک نفوذگر و میدیر شبکه را با بازی معروف موش و گربه و یا یک حمله تروریستی به یک مرکز مهم و حساس کشور مقایسه نمایید. در دنیای واقعی اگر فردی بخواهد به سیستم شما نفوذ نماید وظیفه شما به عنوان مدیر شبکه این است که ازبروز این اتفاق جلوگیری نموده و حملات را بررسی و مشکلات احتمالی سیستم را شناسایی و برطرف نمایید.در این بخش درمورد حملات معمول به شبکه بیشتر صحبت خواهیم نمود.

ابزار نفوذگران : حملات معمول به شبکه

حملاتی که از سمت نفوذگران هدایت می شود حملات از پیش برنامه ریزی شده یا هدایت شده می نامند.به عنوان مثال نفوذ گر با ابزاری که در این بخش با هم بررسی می نماییم اقدام به برنامه ریزی برای نفوذ به سیستم کاربر و با یک سلسله حملات راه را برای رسیدن به مقصود خود هموار می نماید. اما ویروس ها و سایر بد افزار ها تنها از کاربری به کاربر دیگر بر روی بستر اینترنت منتقل می شوند و هدف آنها کاربر خاصی نیست. در این بخش در مورد تکنیک هایی که نفوذگران استفاده می نمایند بیشتر صحبت خواهیم نمود.

کلاهبرداری اینترنتی

این روش روندی است که که طی آن داده ها با آدرس فرستنده جعلی که اینگونه وانمود شود که داده از سمت سیستم اصلی ارسال شده است برای یکی از سیستم های درون شبکه فرستاده می شود تا از این طریق بتوانند به سیستم نفوذ نمایند. مسیریاب داده را همانند یک داده واقعی می بیند و آن را برای گیرنده ارسال می گردد. اما در هنگام عبور داده از دیواره آتش ، هویت جعلی این داده مشخص شده و مانع عبور آن خواهد شد.



اجرای ping تا مرگ سیستم :

این حمله یکی از حملات Denial Of Service)DoS) می باشد.با این کار کاربران حتی اگر مجاز باشند هم امکان ورود و استفاده از منابع را نخواهند داشت. در حالت عادی فرمان ping یکی از ابزار کاربردی شبکه است که با کمک آن می توان مشخص نمود که آیا سیستم در مقابل این در خواست جوابی می دهد یا خیر.در حالت عادی ۴ بسته داده با پروتکل ICMP برای سیستم مقصد ارسال می گردد تا مشخص شود که سیستم مقصد آیا در دسترس می باشد یا خیر اما در این حالت حجم بسته های داده بسیار زیاد شده و همچنین تعداد بسته های ارسالی هم بسیار زیاد می شودتا از این طریق بار سیستم مقصد افزایش یابد و این کار تا هنگ کردن سیستم یا راه اندازی مجدد و در نتیجه قطع کامل ارتباط سیستم با شبکه ادامه پیدا می کند. امروزه بسته های امنیتی به سیستم های عامل اضافه شده است تا از وقوع این حملات جلوگیری شود.

WinNuke

یکی از نرم افزار هایی بود که می توانست بسته هایی با آدرس فرستنده غیر واقعی بر روی شبکه ارسال نماید.این نرم افزار در سیستم های عامل ویندوز نسخه های ۹۵ ؛۹۸ ، NT و ۲۰۰۰ هنگام دریافت اشکالاتی را ایجاد می نمود و سیستم را از دسترس خارج می نماید زیرا سیستم نمی تواند برخوردی مناسب با این داده ها انجام دهد از این رو دچار سر در گمی می گردد. در این حالت سیستم صفحه آبی مربوط به اخطار سیستم را به نمایش می گذارد. این حمله تنها بر روی سیستم عامل ویندوز را مورد حمله قرار می دهد و بر سیستم عامل های دیگر اثری ندارد.

SYN Flood

این نوع حمله هم از ساختار حملات Denial Of Service) DoS)یا حملات قطع سرویس است. در این روش سیستم مقصد با هزاران بسته بی معنا بصورت مسلسل وار مورد حمله قرار می گیرد.در حالت عادی هرگاه سیستم بخواهد بسته ای را با پروتکل TCP/IP ارسال نماید ابتدا یک بسته SYN برای گیرنده ارسال می کند تا ارتباط را برقرار نماید. دیگر نیازی به ارسال این بسته نخواهد بود تا زمانی که ارتباط برقرار باشد و تنها در صورت قطع ارتباط برای برقراری مجدد ارتباط باز هم این بسته ارسال می گردد. اما اگر سیستم مورد حمله قرار گیرد بر اثر ارسال این بسته ها سیستم تمامی ذخایر خود را برای ارایه پاسخ به این بسته ها استفاده می نماید پس از تمام شدن منابع سیستم ، تمامی داده هایی که به سیستم می رسند رد شده و دیگر به سیستم وارد نمی شوند که این داده ها می تواند درخواست های واقعی برای ارتباط و یا هر داده دیگری که از سیستم های دیگر ارسال شده است باشد.بسته های امنیتی که می تواند از وقوع این حملات جلوگیری نماید برای اکثر سیستم های عامل تهیه شده و بر روی آنها نصب شده است.

شناسایی نفوذگران: تکنیک های دفاعی

شناسایی و نفوذ گران و دفاع در مقابل آن به ۳ بخش تقسیم می شود:

- شناسایی فعال : بررسی تمامی داده ها ی شبکه
- شناسایی غیر فعال :ذخیره وقایع امنیتی بر روی یک فایل
- دفاع پیشگیرانه : استفاده از ابزار های مختلف برای ارتقای امنیت ورودی های شبکه در مقابل حملات

شناسایی فعال

شناسایی فعال را می توانیم با یک سرباز که در طول درب ورودی قدم می زند و کاملا تمامی رفت و آمد ها را بررسی می نماید و سعی در کشف رخنه های فیزیکی دارد مقایسه نماییم. نرم افزار های ویژه ای وجود دارد که سیستم را برای رخنه های احتمالی به سیستم بررسی می نماید.این نرم افزار ها با انواع تکنولوژی هایی که نفوذ گران از آنها استفاده می کنند کاملا آشنا هستند و می توانند تمامی فعالیت های مشکوک در شبکه را مشاهده و بررسی نمایند. برخی از نرم افزار های پیشرفته تر توانایی انجام عملیات مختلف مانند قطع ارتباط در هنگام شناسایی حمله و یا ارسال پست الکترونیک برای با خبر کردن مدیر شبکه در زمان حمله به سیستم را هم دارند. NetRanger شرکت Cisco و Snort را می توان نمونه هایی از نرم افزار های شناسایی فعال دانست.

شناسایی غیر فعال

دوربین های امنیتی مدار بسته را می توان یکی از نمونه های شناسایی غیر فعال دانست. تمامی اتفاقات را ثبت نموده و می توان در زمانی دیگرآن را بررسی نمود و به مشکلات رخ داده پی برد.در صورتیکه مدیر شبکه نسبت به وضعیت امنیت شبکه مشکوک باشد به فایل ثبت وقایع مراجعه نموده و می تواند اتفاقاتی که رخ داده را با زمان ورود و خروج کاربران مطابقت داده و آنها را بررسی نموده و در صورت بروز مشکلات آن را برطرف نماید.

دفاع پیشگیرانه

یکی از مشخصات اصلی این ساختار این نکته است که شما اطمینان دارید که شبکه شما در مقابل حملات کاملا ایمن است. انجام این کار با بررسی و تحقیق بر روی نقاط ضعف و قوت شبکه امکانپذیر می شود.البته بایدتمامی اطلاعات به روز باشد و وضعیت فعلی شبکه مد نظر قرار گیرد. شما می توانید با کمک برخی ابزار ویژه مانند satan و یا Port Scanner رخنه های امنیتی شبکه را پیدا نمایید و آن ها را با کمک بسته های افزودنی امنیتی آنها را مسدود نمایید اما این مراحل شاید چندین و چند بار در طول کار هر مدیر شبکه پیش بیاید زیرا شناسایی رخنه و مسدود کردن آن امری که نمی توان برای آن پایانی پیدا کرد و همواره ادامه دارد.

مفهوم رمز نگاری

قبلا هم در این مورد صحبت کردیم که داده های حساس مربوط به افراد ، شرکت ها و سازمان های اداری بر روی بستر اینترنت منتقل می شوند اگر این داده ها با فرمت اصلی خود منتقل شوند امکان قرار گرفتن آن در اختیار افراد غیر مجاز زیاد می شود . برای جلوگیری از بروز این اتفاق داده ها را رمز نگاری می نمایند تا اگر در بین راه کسی به این داده ها دسترسی پیدا کند داده ها برای این فرد مفهوم نبوده و از این داده ها نمی تواند استفاده نماید.داده هایی که رمز نگاری شده زمانی که به مقصد رسید رمز گشایی می شود و قابل استفاده برای گیرنده می شود.داده ها توسط یک الگوریتم خاص که به آن کلید یا Key می گویند رمز نگاری یا Encrypt می شود و در زمان رسیدن به مقصد داده هارمز گشایی یا Decrypt می شود.

رمز نگاری کجا استفاده می شود؟

در بسیاری از موارداستفاده از رمز نگاری بسیار ضروری است.ارسال کلمه عبور کاربر برای سرور باید رمز نگاری شده باشد. این کار بصورت خودکار توسط سیستم های عامل امروزی انجام می گیرد. برخی از ابزار کاربردی مانند FTPوTelnet از رمز نگاری پشتیبانی نمی نمایند و کلمه عبور را بصورت عادی ارسال می نماید. خرید محصولات و پرداخت مبلغ آن از طریق حساب بانکی باید رمز نگاری شده باشد در غیر اینصورت اطلاعات حساب بانکی کاربر ممکن است در اختیار دیگران قرار گیرد و ضرر مالی فراوانی به کاربر بزند.

رمز نگاری چگونه کار می کند؟

پروسه رمز نگاری داده ها در واقع مراحلی است که طی آن هر کاراکتر از یک کلمه تبدیل به عبارتی دیگر بر اساس کلید رمز نگاری می شود.به عنوان مثال شما می توانید این عبارت را رمز نگاری نمایید:

این عبارت یک جمله آزمایشی است.

برای بحث آموزشی خود از ساده ترین روش که تبدیل حروف به اعداد است استفاده می نماییم.در این روش یک عدد به هر حرف از حروف الفبا نسبت داده می شود .مثلا با کمک جدول زیر که در واقع کلید رمز نگاری می باشد می توانیم عبارت بالا را تبدیل نماییم:

کاراکتر	معادل عددی	کاراکتر	معادل عددی
الف	۱۲	ش	۷
ی	۹	س	۱۶
ک	۳	ت	۴
ج	۱۱	ع	۸
م	۱۹	ب	۶
ل	۱۰	ر	۲۰
ه	۱	ن	۲
ز	۵		

معادل عددی عبارت به این صورت خواهد شد.

۱۲ ۹ ۲ ۸ ۶ ۱۲ ۲۰ ۴ ۹ ۳ ۱۱ ۱۹ ۱۰ ۱ ۱۲ ۵ ۱۹ ۱۲ ۹ ۷ ۹ ۱۲ ۱۶ ۴

البته این ساده ترین ساختار رمز نگاری است. تکنولوژی هایی که در حالت واقعی استفاده می شود بسیار پیچیده تر از این ساختار هستند که نمی توان آن را به راحتی کشف نمود.

کلید های رمز نگاری

برای رمز نگاری و رمز گشایی هر پیام شما نیاز به یک کلید مناسب دارید.این کلید می تواند یک فرمول و یا مانند مثال ما یک جدول باشد که نحوه تبدیل کاراکتر ها را به رمز را مشخص می نماید. این کلید به ۲ گروه تقسیم می شود: خصوصی و عمومی

در این بخش ما در مورد این دو نوع کلید بیشتر صحبت خواهیم نمود.

کلید خصوصی رمز نگاری

این کلید همچنین با نام کلید متقارن (Symmetrical Key) هم معروف است. در ساختار کلید خصوصی هر دو سمت گیرنده و فرستنده یک کلید یکسان دارند و از آن برای رمز نگاری و رمزگشایی استفاده می کنندالبته این روش تنها یک عیب دارد و آن هم برقراری ارتباط برای بار اول است زیرا این کلید باید در هر دو سمت وجود داشته باشد و ارسال این کلید برای طرف دوم یک مشکل عمده است .برای این انتقال شما باید از کلید های عمومی در شبکه استفاده کنید.که در مورد آن هم صحبت خواهیم نمود.

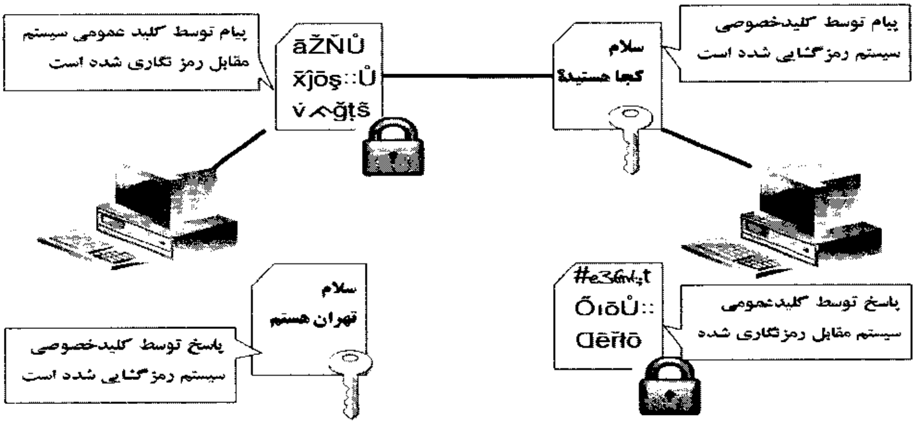
استاندارد رمزنگاری داده ها (DES)

برای اولین بار استاندارد مربوط به رمز نگاری داده ها توسط شرکت IBM طراحی شد.پس از آن در سال ۱۹۷۷ دولت آمریکا این استاندارد را تایید نمود وپس از آن اجرایی گردید.

استاندارد رمز نگاری از یک جدول رمز استفاده می کند از این رو بسیار سریعتر از کلید های عمومی عمل می نماید.در یک کلید ۵۶ بیتی خصوصی میزان احتمالات در این حالت ۷۲ کوآدریلیون حالت خواهد شد. در سال ۱۹۹۷ پس از تلاشی چندین ساله الگوریتم این رمز بالاخره شکسته شد و محتویات آن قابل خواندن گردید.

کلید عمومی رمز نگاری

کلید عمومی یا الگوریتم Diffie-Hellman از ۲ کلید برای رمز نگاری و رمز گشایی استفاده می نماید.در زمان ارسال به گیرنده کلید عمومی برای رمزنگاری داده ها استفاده می شود. هنگامی که داده به مقصد رسید ، گیرنده آن را با کلید خصوصی خود رمز گشایی می نماید.این روش یک ارتباط یک طرفه است. این روال می تواند کاملا به همین صورت برای دریافت پاسخ هم تکرار می شود. در تصویر زیر شما این ساختار را مشاهده می نمایید.



حفظ حریم خصوصی

(PGP)Pretty Good Privacy یک ابزار رمز نگاری است که بر پایه کلید عمومی کار می کند.از ابتدا این ابزار برای رمز نگاری پست الکترونیک استفاده می شد.پست الکترونیک را می توان با کارت پستال مقایسه کرد. این کارت در طول مسیر بین فرستنده تا گیرنده قابل مشاهده توسط تمامی افراد است و هیچ مساله ای خصوصی نمی توان در آن نوشته شود.برای رفع این مشکل باید نوشته ها به رمز نوشته شود. انتقال یک کارت پستال بصورت امن را می توان با ارسال آن درون یک پاکت در بسته مقایسه نمود. البته به مرور زمان امروزه کمتر از این گونه ابزار استفاده می شود.

سیاست های امنیتی

سیاست های امنیتی در واقع قوانین امنیتی است که بر شبکه شما حاکم است که شامل امنیت فیزیکی ،امنیت منابع و امنیت شبکه می شود. این سیاست باید بصورت یکسان بر روی همه بخش های شبکه اجرا شود.در غیر این صورت امنیت شبکه شما مانند یک صفحه شطرنج است برخی نقاط امن است و برخی نقاط دارای رخنه است.برای داشتن یک شبکه امن قبل از هرچیز باید سیاست های امنیتی شبکه مشخص شده و به اطلاع کاربران برسد همه کاربران باید مطابق این سیاست ها رفتار نمایند تا امنیت شبکه تامین شود.

بازرسی امنیتی

بازرسی امنیتی یک بررسی کامل شبکه است تا با کمک آن نقاط ضعف شبکه آشکار شود. شما می توانید خود این بررسی را انجام داده و یا قراردادی با شرکت ها و یا کارشناسان دیگر انجام دهید.اگر تصمیم داشته باشید امنیت شبکه خود را ضمین نمایید این بهترین گزینه برای شماست.زیرا یک ناظر بیرونی بسیار بهتر از یک کاربر داخل شبکه است زیرا دید ناظر نسبت به کاربر بسیار وسیع تر است. این کار معمولا توسط شرکت های معتبر و مجاز انجام می شود و پس از اتمام کار یک گواهی تاییدیه امنیتی به شما اعطا می شود.

بسیاری از سازمان های دولتی قبل از هر قراردادی با شما به دلیل حساسیت قرارداد های اجرایی خود ، یک تاییدیه امنیتی از شما می خواهند که توسط شرکت های مجاز صادر شده باشد.

میز کار تمیز

این سیاسیت امنیتی به این معنی نیست که میز کار هر کاربر تمیز شده و هیچ گرد و غبار و یا باقیمانده غذا بر روی آن باقی نماند.بلکه هدف از این کار ساماندهی نامه ها و برگه های اداری روی میز هر کاربر است این

برگه ها باید از روی میز جمع آوری شده و در محلی محفوظ نگهداری شود. زمانی که کاربر نامه های اداری را بر روی میز خود رها می کند ممکن است هر فردی نامه ها را بدون اجازه بر دارد.اگر این نامه محرمانه باشد می تواند امنیت سازمان شما را بصورت جدی به خطر بیندازد.با تمیز کردن و برداشتن نامه ها از روی میز می توان از بروز این خطرات جلوگیری نمود.

طبق بررسی های به عمل آمده منشا تقریبا۸۰ درصد نفوذ های شبکه کارمندان ساز مان و کاربران همان شبکه هستند که از شبکه داخلی برای نفوذ استفاده می نمایند. شاید استفاده از دیواره آتش تازه آغاز کار شما برای برقراری امنیت در شبکه است .

برای اینکه این سیاست مفید باشد باید برای کاربر عادت شود که هیچگاه بدون جمع آوری اسناد و مدارک میز کار خود را حتی برای چند دقیقه هم ترک ننماید.زیرا حتی اگر یکبار هم این اتفاق بیفتد می تواند لطمات جبران ناپذیری به سازمان و شبکه شما وارد نماید.

ابزار ثبت و ضبط

ابزار ضبط می تواند نوار مغناطیسی یا و یادوربین های ویدیویی باشد که حاوی اطلاعات حساس شخصی یا اداری باشد.سیاست های امنیتی شما می تواند شامل محدودیت استفاده از این تجهیزات باشد.زیرا می توان با یک دوربین بسیار کوچک از تمامی اسناد و مدارک مهم تصویر برداری نمود و از آن برای مقاصد ویژه مانند جاسوسی استفاده نمود. نحوه برخورد شما با اینگونه تجهیزات می تواند میزان امنیت شبکه شما را مشخص نماید. این تجهیزات می تواند شامل حافظه های جانبی USB که امروزه بسیار همه گیر شده است هم باشد.

در بسیاری از سازمانها و شرکت ها از ورود این تجهیزات جلوگیری می نمایند و محل نگاهداری تجهیزات را توسط دوربین های امنیتی به شدت کنترل می نمایند زیرا برخی از این حافظه ها در مقیاس بسیار کوچک ساخته شده اند و یا در برخی وسایل دیگر مانند ساعت جاسازی شده اند که تشخیص آنها را مشکل می سازند و با بررسی تصاویر دوربین ها می توان از دسترسی غیر مجاز به منابع جلوگیری نمایید.

برخی از سیاست های امنیتی متداول

اطلاع رسانی

آیا فکر می کنید یک سیاست امنیتی خوب آن است که کسی از آن خبر نداشته باشد ؟اگر زمانی که کاربری به شبکه شما وارد می شود به همراه اطلاعات حساب کاربری یک نسخه از سیاست ها ی امنیتی شبکه را هم دریافت نماید می تواند با مواردی که باید رعایت نماید آشنا شود. همچنین می توان یک اخطار مانند "دسترسی بدون مجوز ممنوع بوده و پیگرد قانونی دارد. " برای کاربر به هنگام اتصال به شبکه نمایش داده شود و کاربر با تایید مشاهده پیام امکان اتصال به شبکه را داشته باشد این کار می تواند علاوه بر اخطار حکم تایید قوانین شبکه توسط کاربر باشد .

دسترسی به تجهیزات

غیر فعال کردن درگاه هایی که مورد استفاده قرار نمی گیرند در تجهیزات شبکه باعث می شود که افرادی که کاربر شبکه نیستند اگر بصورت تصادفی وارد محیط کاری شبکه شما شوند نتوانند به شبکه متصل و یا از منابع شبکه شما استفاده نماید. همچنین محل نگهداری تجهیزات باید از نظر فیزیکی کاملا محفوظ باشد و توسط دوربین کنترل شود.

کابل کشی

کابل های شبکه باید در راستای دیوار و نزدیک کف باشد تا دسترسی به آن راحت باشد.مسیر یاب ، مودم و یا سوییچ هیچگاه نباید در محیط باز قرار بگیردو حتما باید در رک و اتاق در بسته تحت شدیدترین تدابیر امنیتی نگهداری شود.

قفل درب ورودی

تمامی محل های نگهداری سرور ها و تجهیزات شبکه همچنین دیتا سنتر ها باید مجهز به مکانیزمی باشند که تنها امکان ورود کاربران خاصی به فضا ی دیتا سنتر و اتاق سرور فراهم شود این مکانیزم می تواند اسکنر اثر انگشت ،کارت الکترونیکی یا کد عبور باشد. باید تمامی کاربران مجاز به خاطر داشته باشند که هیچگاه درب را بدون نظارت حتی برای لحظه ای باز نگذارند.

کارت هویت

یکی از موارد مهم وجود کارت شناسایی است که افراد آن را همیشه بر روی لباس خود نصب نمایند این کارت می تواند مشخص کند که فرد کارمند یا میهمان است و همچنین سطح دسترسی کاربر هم در آن مشخص می شود. این کارت می تواند امنیت فیزیکی شبکه را ارتقا دهد زیرا کاربران غیر مجاز هیچگاه نمی توانند به مکان

های حساس وارد شوند همچنین کاربران در صورت ورود به مکان های خاص می توان زمان ورود و خروج آنها را برای بررسی های بعدی ثبت نمود.

کلمه عبور

همانگونه که قبلا هم ذکر نمودیم کلمه عبور باید در دوره های زمانی تغییر نماید این دوره زمانی بستگی به سیاست های امنیتی شما دارد . بطور معمول این زمان حداقل ۳۰ روز است. همچنین باید کلمه عبور BIOS هم تغییر نماید تا کسی نتواند بطور از این طریق در سیستم خرابکاری ایجاد نماید.

زاویه دید نمایشگر

نمایشگر ها را باید بصورتی تنظیم نمود که میهمان نتواند محتویات صفحه کاری شما را از طریق نمایشگر ببیند.باید مطمئن باشید که افراد غیر مجاز نمی توانند نمایشگر سرور ها و دیگر سیستم ها را مشاهده کنند.این موارد در مورد خروجی چاپگر و یا دورنگار هم صادق است.

حساب کاربری

هر کارمند مجموعه شما باید یک حساب کاربری مخصوص به خود داشته باشد.حتی کاربرانی که بصورت پاره وقت و یا پروژه ای به شبکه شما وارد می شود باید حساب کاربری برایشان تعریف شود . شما با این کار می توانید بر وضعیت شبکه خود نظارت داشته باشید. در بین مدیران شبکه گاهی مشاهده می شود که تعدای حساب کاربری میهمان دارند و در صورت ورود یک کاربر میهمان یا پاره وقت به شبکه از آن حساب کاربری استفاده می نماید. این کار اصلا توصیه نمی گردد زیرا امکان بررسی مشکلات ،حملات و یا سوء استفاده های احتمالی را بگیرد.

بررسی سوابق

این کار شامل ۲ بخش است. برای هر کارشناس و یا مدیر که به سیستم شما وارد می شود از یک جهت باید سوابق علمی ،تحصیلی وکاری گذشته مورد بررسی قرار گیرد و از سوی دیگر عدم سوء پیشینه و عدم اعتیاد به مواد مخدر هم لازم وضروری است.این کار باعث می شود افراد سالم و مناسب به کادر اجرایی شبکه شما وارد شود.

دیواره آتش

استفاده از یک دیواره آتش مناسب برای امنیت کاربران شبکه اینترنت در کنار یک سرور پروکسی می تواند امنیت قابل قبولی را برای شبکه شما فراهم آورد.البته امکانات دیواره آتش بستگی به امکانات مورد نظر شما ، سیاست های امنیتی و البته بودجه شما دارد.

شناسایی نفوذگران

سیستم شناسایی نفوذگران ویک سیستم ثبت وقایع می تواند کمک بسیاری به شما جهت افزایش امنیت شبکه نماید. با کمک این ساختار شما می توانید تمامی حملات به سیستم را شناسایی وبا اجرای راه حل های مناسب امنیتی نقاط ضعف شبکه را برطرف نمایید.

دوربین های امنیتی

دوربین های امنیتی باید تمامی نقاط ورودی و خروجی ،اتاق سرور و همینطور پارکینگ های ساختمان را پوشش دهد.دوربین هایی که در فضای باز قرار می گیرند باید دارای پوشش محافظ بوده که نسبت به عوامل محیطی مقاوم باشد.تصاویر این دوربین ها باید توسط نگهبان های امنیتی مشاهده شود و برای مدتی معین ذخیره شود تا در صورت بروز مشکل بتوان با کمک آن مقصر را شناسایی نمود.

پست الکترونیکی

هر شبکه باید یک سرور پست الکترونیکی داشته باشد که به حساب هر کاربر متصل باشد.با وجود این سرویس می توان فعالیت های هر کاربر را مورد بررسی قرار داده و امکان خروج اطلاعات از شبکه را غیر ممکن سازید.البته ذکر این نکته لازم است که در این صورت استفاده از سرویس های پست الکترونیکی عمومی برای کاربران غیر مجاز خواهد بود.

DMZ

همانگونه که قبلا در این مورد صحبت نمودیم تمامی سرور هایی که از بیرون شبکه به آنها دسترسی وجود دارد باید در این محیط قرار گیرند. اگر سرور ها خارج از این محیط و بیرون از محیط دیواره آتش قرار گیرند امنیت آنها به شدت مورد تحدید قرار می گیرد.

بسته های افزودنی

شما همیشه باید اطمینان داشته باشید که همیشه سیستم به روز باشد و آخرین بسته های امنیتی بر روی سیستم نصب شود.البته توصیه می شود همیشه بسته های امنیتی ابتدا بر روی یک سیستم نصب شده و آزمایش شود در صورتیکه اثری منفی بر سیستم نداشت یر روی سرور ها و دیگر سیستم های شبکه نصب گردد.

پشتیبان

در مورد تهیه پشتیبان و ساختار های آن در مباحث گذشته صحبت نمودیم. در این بخش در مورد نحوه ذخیره پشتیبان ها صحبت می نماییم. پشتیبان ها باید در محیطی کاملا امن نگهداری شود. این محل امن باید در مقابل آب و آتش ایمن بوده و کاربران غیر مجاز نتوانند به آن دسترسی داشته باشند.توصیه می گردد این مکان خارج از محیط نگاهداری سرور ها باشد.

مودم ها

به هیچ عنوان اجازه استفاده از مودم را به کاربران شبکه ندهید زیرا می توانند بدون اطلاع شما به اینترنت متصل شوند و اطلاعاتی از شبکه شما خارج و یا برخی نرم افزار های مخرب به شبکه شما وارد نمایند.

نگهبانان امنیتی

در بسیاری از موارد وجود نگهبانان امنیتی لازم و ضروری است.زیرا در برخی موارد تنها تصویر دوربین امنیتی نمی تواند جلوی نفوذ به شبکه یا انجام خرابکاری را بگیرد . ممکن است شما بخواهید قبل از وقوع از بروز یک مشکل جلوگیری نمایید اینجاست که شما نیاز به نیروی انسانی دارید.

جریمه شکستن قوانین امنیتی سیستم

هیچ قانونی در شبکه اجرا نمی شود مگر آنکه کاربران مجبور به اجرای آن باشند.اگر شما برخی از کاربران را از اجرای قوانین معاف نمایید راهی را برای عدم اجرای قوانین توسط دیگران هموار نموده اید.شما باید بصورت کاملا روشن و شفاف به کاربران اعلام کنید که مجاز به انجام چه کار هایی هستند و انجام چه کار هایی برای آنها ممنوع است. همچنین باید برای کاربران مشخص شود که جریمه شکستن قانون و عدم اجرای هر یک از قوانین چه خواهد بود.این کار می تواند هزینه قانون شکنی را افزایش داده و کمتر کسی به این کار دست خواهد زد.

تخلف عمده

در سال های گذشته کاربر در صورت تخلف از قوانین اخراج می شد. حال این تخلف می توانست کوچک باشد یا بزرگ تفاوتی وجود نداشت زیرا تقسیم بندی برای انواع خطا ها و جریمه هر کدام صورت نگرفته بود.برای جلوگیری از این کار باید بصورت شفاف و مشخص تخلفات عمده و جریمه آنها برای کاربر ذکر شود. با این کار دیگر کاربر هیچگاه بصورت عمدی مرتکب این تخلفات نمی شود و اگر هم بصورت غیر عمدی این اتفاق افتاد جریمه آن کمتر خواهد بود.

تخلف جزیی

تخلفات جزیی می تواند عمدتا بصورت تصادفی اتفاق افتد.با نصب یک نرم افزار بر روی سیستم ممکن است سیستم عامل دچار اختلال شود و نیاز به ترمیم نرم افزاری وجود داشته باشد. نسخه های نمایشی نرم افزار ها و بسته های امنیتی قبل از نصب بر روی سیستم ها باید آزمایش شود پس از آن بر روی سیستم ها نصب شود. هیچ کاربری را برای تخلفات جزیی از شبکه اخراج نمی نمایند و تنها با برخی جریمه های جزیی می تواند به فعالیت خود در شبکه ادامه دهد.

مصاحبه هنگام خروج

در شرکت های بزرگ کارفرما هنگام خروج هر کاربر از سیستم با او مصاحبه ای انجامی می دهد و در مورد تجربیات و خاطرات خود در زمان حضور در شبکه با او صحبت می کند. این کار باعث می شود که کاربران مشکلات خود رامطرح کنند تا اگر کاربر علاقه به حضور در سازمان دارد و حضور او برای شبکه مفید است مانع رفتن او شوند و یا ممکن است کاربر دلخوری هایی داشته باشد که قبل از رفتن از او دلجویی شود تا بخاطر کینه در آینده به سیستم ضربه ای نزد.

بررسی اموال باقیمانده از کاربر

پس از خروج هر کاربر از سازمان شما ؛کاربر لوازم شخصی خود را با خود می برد. سپس باید تمامی اموالی که در زمان کار در اختیار او قرار داشته است مورد بررسی قرار گیرد و کلمه عبور سیستم و تمامی کد های امنیتی که کاربر به آنها دسترسی داشته است باید تغییر نماید و خروج او به تمامی نگهبانان امنیتی هم اطلاع داده شده و از ورود او جلوگیری شود.

در خصوص برخی از کاربران با دسترسی های ویژه مانند مدیران شبکه لازم است بلافاصله دسترسی آنها به سیستم غیر فعال شده و ورود فرد به اتاق سرور و دیگر بخش های حیاتی و مهم شبکه ممنوع شود و این ممنوعیت به اطلاع تمامی نیروهای امنیتی و نگهبانان برسد. اما در مورد کاربران با سطح دسترسی پایین تر این اقدامات پیشگیرانه را می توان کمی به تعویق انداخت و ضرورتی برای انجام آن با سرعت نیست.

جمع بندی:

در این بخش شما:

- ❖ درخصوص ساختار های امنیتی مختلف و نحوه اجرای آنها در شبکه مطالب مهمی آموختید.
- ❖ انواع ساختار های مختلف دیواره آتش را بررسی نموده و در مورد سیستم عامل های آن هم بصورت تفصیلی صحبت نمودیم.
- ❖ با عملکرد دیواره آتش و نیاز به وجود آن در شبکه آشنا شدید.
- ❖ در مورد سرور پروکسی و انواع ساختار های آن صحبت نمودیم.
- ❖ در خصوص رمز نگاری و ساختار های آن صحبت نمودیم.

سوالات ارزیابی برای آزمون Network+ :

۱ –کدامیک از این تجهیزات به عنوان نماینده کاربران شبکه درخواست های آنها را از اینترنت دریافت می نماید.

الف) پست الکترونیکی

ب) پروکسی

ج) لیست کنترل دسترسی

د) سرور FTP

۲-کدامیک از این سیستم عامل های می تواند در دیواره آتش مورد استفاده قرار گیرد..(تمامی موارد صحیح را مشخص نمایید)

الف) ویندوز

ب) یونیکس

ج) لینوکس

د) ناول

۳-کدامیک از این حملات تنها بر روی کاربران سیستم عامل ویندوز اثر دارد.

الف) SynFlood

ب) WinNuke

ج) Ping تا مرگ سیستم

د) SynNuke

۴- توصیه شده که کاربر باید حداکثر چه مدت یکبار کلمه عبور خود را عوض کند.

الف) هیچوقت

ب) هر روز یک بار

ج) هر ماه یک بار

د) هر سال یک بار

۵-کدامیک از این کلمات عبور به عنوان کلمات عبور ضعیف شناخته می شود. (تمامی موارد صحیح را مشخص نمایید)

الف) ali110

ب) Password11

ج) PQ@y57!=b

د) 1288539871566

۶- کدامیک از این محل ها برای نگهداری پشتیبان ها مناسبترین محل است .(تمامی موارد صحیح را مشخص نمایید)

الف) کشوی میز مدیر شبکه
ب) کمدی در اتاق سرور
ج) گاو صندوق در اتاق مدیر شبکه
د) در یک گاو صندوق خارج از محیط شبکه

۷- ازتصاویر دوربین امنیتی می توان در چه مواردی استفاده نمود . (تمامی موارد صحیح را مشخص نمایید)

الف)کنترل کاربران هنگام ورود و خروج از دیتا سنتر.
ب) کنترل کاربران خدماتی برای نظارت بر نحوه تمیز نمودن محل
ج) ورود و خروج کاربران و میهمانان به داخل محیط اداری
د) نظارت بر ترافیک خیابان های اطراف

۸-کدامیک از این اسامی بهترین انتخاب برای نام کاربری مدیر شبکه است . (تمامی موارد صحیح را مشخص نمایید)

الف) Administrator
ب) admin
ج) bholmes
د) Nimda

۹- کدامیک از این موارد می تواند مشخصات یک کلمه عبور قوی را بیان نماید. (تمامی موارد صحیح را مشخص نمایید)

الف) طول آن بیشتر از ۱۵ کاراکتر باشد.
ب) حدس زدن آن مشکل باشد اما به خاطر سپردن آن آسان باشد.
ج) از زبان اصلی سیستم در آن استفاده نشود.
د) ترکیبی از حروف ، اعداد و کاراکتر های خاص باشد.

۱۰-به همراه داشتن کدامیک از ابزار ذخیره سازی در شبکه های بزرگ مجاز نیست. (تمامی موارد صحیح را مشخص نمایید)

الف) دوربین های عکاسی کوچک
ب) ضبط صوت های کوچک
ج) حافظه های جانبی USB
د) دوربین های کوچک ویدیویی

پاسخ به سوالات این بخش

۱ - ب

همانگونه که در مطالب این بخش ذکر شده سرور پروکسی به عنوان نماینده کاربران شبکه درخواست های آنها را از اینترنت دریافت می نماید و در اختیار آنها قرار می دهد و مانع ارتباط مستقیم کاربران با اینترنت می شود.

۲ - الف ، ب ،ج ،د

تمامی سیستم های عامل ذکر شده می توانند در ساختار دیواره آتش مورد استفاده قرار بگیرند.

۳ - ب

با توجه به توضیحات این فصل مشخص است که تنها این حمله محدود به کاربران ویندوز است و حملات دیگر در تمامی سیستم های عامل یکسان است.

۴ - ج

توصیه شده است که این کار هر ماه انجام گیرد.

۵ - الف ، ب ،د

گزینه اول به دلیل کوتاه بودن طول این کلمه و همچنین استفاده از نام های مذهبی در آن ،گزینه گزینه دوم استفاده از کلمه password و گزینه آخر به دلیل استفاده تنها از اعداد کلمات عبور ضعیف هستند.

۶ - ج،د

پشتیبان باید در جایی امن نگهداری شود. البته توصیه شده است که در جایی خارج از محیط شبکه نگهداری شود.

۷ - الف ،ج

از این دوربین ها تنها برای کارهای امنیتی استفاده می شود و نباید برای امور خدماتی و یا تفریحی استفاده نمود.

۸ - ج

گزینه های دیگر از اسامی غیر مجاز است.

۹ - **ب ،د**

کلمه عبور بین ۸ تا ۱۵ کاراکتر است. و اگر از زبان سیستم استفاده نشود برای ورود آن به سیستم دچار مشکل خواهیم شد.

۱۰ -**الف ، ب ،ج ،د**

کاربران مجاز به همراه داشتن هیچکدام از این ابزار نیستند.زیرا امنیت شبکه را به خطر می اندازد.

فصل نهم

اومت در برابر بروز خطا و بازیابی آن



شما در این فصل با این مفاهیم آشنا خواهید شد:

۹-۱ شناسایی اهداف، مزایا و خصوصیات نرم افزار های شناسایی و مقابله با اثرات ویروس ها :

۹-۲ شناسایی اهداف ، مزایا و خصوصیات مقاومت در برابر خطا :

- ❖ مشکلات انرژی
- ❖ خطوط جایگزین
- ❖ ابزار ذخیره سازی
- ❖ سرویس ها

۶- ۳ شناسایی عملکرد و خصوصیات سیستم های بازیابی خطا ها

- ❖ پشتیبان گیری و بازگرداندن آن
- ❖ ذخیره سازی در خارج از مجموعه
- ❖ جایگزینی سیستم ها
- ❖ طرح های سایت گرم ،ملایم و سرد

مقدمه:

رایانه ها ابزاری بدون اشتباه نیستند و احتمال بروز خطا در هنگام استفاده از آنها بسیار زیاد است.این خطا ها می توانند اشکالات سخت افزاری یا نرم افزاری باشند. منشا این خطا ها می تواند بلاهای طبیعی ؛ نوسانات برق یا خرابکاری توسط نرم افزار های مخرب باشد.

یکی از وظایف اصلی مدیر شبکه پیشگیری از بروز خطا در شبکه است. این اقدامات هم از بروز خطا پیشگیری نموده و هم می تواند سیستم را به حالت عادی باز گرداند.در این بخش ما با دو مفهموم آشنا می شویم:

- Fault Tolerance
همانگونه که از نام آن مشخص است توانایی مقاومت در برابر بروز خطاست به این معنی که سیستم در صورت بروز خطا و مشکل از فعالیت دست بر نداشته و مشکلات را هم می تواند برطرف نماید تا سیستم یا شبکه بتواند همیشه به فعالیت خود ادامه دهد.
- Disaster Recovery
در این ساختار توانایی سیستم برای از سر گیری فعالیت در صورت بروز مشکل یا خرابی در حداقل زمان ممکن تضمین می گردد .

در این بخش ما در مورد این سرفصل ها صحبت خواهیم نمود.

- چگونگی سنجش نیاز ها برای اجرای برنامه های مقاومت در برابر بروز خطا و ادامه فعالیت
- مدیریت انرژی
- مدیریت داده ها و سیستم های ذخیره سازی
- پشتیبان گیری
- جلوگیری از نرم افزار های مخرب و ویروس

دانستن این موارد و اجرای آن برای تمامی مدیران شبکه و تمامی کسانی که می خواهند در آزمون Network+ شرکت نمایند لازم است.

چگونگی سنجش نیاز ها برای اجرای برنامه های مقاومت در برابر بروز خطا و ادامه فعالیت :

بر اساس اینکه مدیریت بازیابی خطا چگونه برنامه ریزی شده است ؛ ۳ برنامه تعریف می شود که عبارتند از گرم ؛ ملایم و سرد.هرچه به سمت گرم برویم امکان بروز اختلال در سیستم کم تر می شود.

سایت گرم :

تمامی رایانه ها و دیگر اجزای شبکه در این ساختار دارای حد اقل یک جایگزین هستند. این ساختار در مواقعی مورد استفاده قرار می گیرد که سیستم می بایست ۱۰۰ درصد در دسترس باشد.

با بکار بردن این روش زمان های قطعی در سیستم به صفر می رسد و سیستم ها در تمام مدت مشغول بکار می باشند. تکنولوژی دسته بندی (Clustering) از این ساختار استفاده می نمایند . سیستم ها برای پیشگیری از بروز خطا و افزایش کار آیی سیستم دسته بندی می شوند. دسته بندی معمولا تنها در مورد سرور ها انجام می گیرد. زیرا رایانه ها ارزان هستند و براحتی می توان آنها را جایگزین نمود.

۲ سطح دسته بندی وجود دارد :Failover و True Clustering

:Failover

در این ساختار معمولا ۲ سرور وجود داردیک سرور اصلی است که پاسخگوی نیاز های کاربران است و سرور دیگر سرور در هنگام بروز خطاست.این سرور دقیقا یک نسخه کاملا یکسان از سرور فعال است اما در حالت آماده به کار بوده و کاملا آماده فعال است.این دو سرور توسط یک ارتباط پر سرعت به شبکه متصل هستند .بین دو سرور ارتباطی خاص وجود دارد بدین صورت که سرور ها در زمانی مشخص خبر سلامتی خود را به دیگری اعلام می نماید. اگر در این زمان معین خبر سلامتی به سرور جایگزین سرور اصلی نرسد، بلافاصله جایگزین سرور اصلی شده و وظایف آن را انجام می دهد.شما می توانید در طول این زمان فعالیت های سرور اصلی را بررسی نمایید.

هرگاه سرور اصلی به مدار بازگشت این سرور به حالت آماده باش بر می گردد و پاسخ درخواست های کاربران توسط سرور اصلی داده خواهد. در این ساختار فعالیت سرور تقریبا بدون وقفه ادامه پیدا می کند.

برای این منظور یک نرم افزار مدیریت دسته بندی باید بر روی سرور ها نصب گردد.این نرم افزار بر روی سیستم عامل های ناول و ویندوز وجود دارد. این نرم افزار بر روی ویندوز ۲۰۰۰ و بالاتر فعال می شود و می تواند فعالیت بدون وقفه شبکه را تضمین نماید.

دسته بندی واقعی (True Clustering) :

این روش با روش قبلی دو تفاوت عمده دارد:

- از تعداد زیادی دستگاه پشتیبانی می نماید.
- امکان برقراری توازن بار بین سرور ها (Load Balancing) را فراهم می آورد.

در این روش تعداد زیادی سرور با هم یک گروه را تشکیل داده و در حکم یک سوپر سرور یا یک سرور بسیار بزرگ عمل می نمایند.در این روش بین تمامی سرور ها یک شبکه با سرعت بالا برقرار است و بین آنها توازن بار

ایجاد شده است یعنی تمامی سرور ها بار یکسانی را تحمل می نمایند.هرگاه سروری دچار اختلال شود سرور های دیگر بار آن را بطور مساوی بین خود تقسیم می نمایند تا سرور دوباره به فعالیت عادی خود ادامه دهد.این کار باعث می شود که زمان اختلال در سرور ها بسیار پایین آمده و به نزدیک صفر برسد و عملکرد آنها بسیار بالا برود.

برخی مزایای این روش به این ترتیب است :

- در این روش سرویس های شبکه تقریبا ۹۹ درصد قابل دسترس هستند .زیرا به دلیل سرور های متنوع درصورت بروز مشکل در یک سرور سرور های دیگر وظایف آن را هم انجام می دهند.
- کارآیی و کیفیت به دلیل استفاده از سرور های متعدد بسیار بالاست زیرا هر سرور تنها بخشی از بار شبکه را برعهده می گیرد.
- زمان قطعی سرویس ها در این ساختار تقریبا به صفر می رسد.
- تعدادی از سرور ها می توانند در خارج از مجموعه باشند تا در صورت بروز حوادث غیر مترقبه هم سیستم بتواند با کمک آن سرورها به فعالیت خود ادامه دهد.

در کنار این محاسن این روش معایبی هم دارد :

- بسیاری از نرم افزار های مدیریت دسته بندی حد اکثر ۶۴ سرور و حداقل ۲ سرور را پشتیبانی می نمایند.
- این روش بسیار گران است و بسیاری از شبکه ها توان این هزینه را ندارند و ترجیح می دهند بجای صرف هزینه هنگفت یکروز سرور ها از دسترس خارج شوند.

سایت ملایم :

در این روش سرویس های شبکه در اکثر مواقع قابل دسترس هستند .معمولا سرویس هایی که در این ساختار فعال هستند اهمیت سرویس ها در سایت گرم را ندارند.بر خلاف سایت گرم که تمامی کار ها خودکار بوده و توسط سیستم عامل مدیریت می شوند این ساختار نیاز به اندکی نظارت و مدیریت دارند همچنین ارزانتر هستند زیرا داشتن یک سرور بسیار کم هزینه تر از داشتن جایگزین برای تمام اجزاست.یکی از موارد استفاده از این ساختار سرور های جایگزین هستند.

این سرور ها همانگونه که از اسمشان مشخص است در حال حاضر کاری انجام نمی دهند. استفاده آنها مربوط به زمان بروز اختلال در سرور اصلی است که این سرور ها جایگزین سرور اصلی می گردد. این جایگزینی معمولا تا آماده شدن سرور اصلی ادامه پیدا می نماید.سپس این سرور به محل قبلی خود منتقل می شود.با این روش زمان قطعی سرویس به حداقل ممکن کاهش پیدا می نماید.

معمولا شبکه های بزرگ از این ساختار استفاده نمی نمایندزیرا :

- شما می بایست هر روز از سیستم پشتیبان تهیه نمایید .سپس آن را بررسی نموده تا مشکلی نداشته باشد زیرا تمام ساختار شما بر اساس همین پشتیبان برنامه ریزی خواهد شد که این روندی وقت گیر است.
- امکان از دست دادن داده ها بسیار زیاد است.زیرا اگر شما بعد از ظهر دچار مشکل شوید و نسخه پشتیبان شما مربوط به بعد از ظهر روز گذشته باشد شما داده های یک روز را کاملا از دست می دهید. البته اگر سرور شما به روز نمی شود مشکل زیادی برای شما بوجود نمی آید.

سایت سرد:

این ساختار فعال بودن سیستم را نمی تواند تضمین نماید. در این روش در صورت بروز خطا در سرور کارشناس شبکه سعی می نماید که این خطا را برطرف نماید. اگر قطعه ای نیاز به تعویض داشته باشد سرور تا زمان تعویض آن خاموش می ماند.پیش بینی برای خطاها و مشکلات انجام نمی گردد و در زمان بروز خطا سعی برای رفع آن آغاز می گردد.

این روش تنها یک مزیت دارد و آن هم ارزان بودن این روش است.زیرا هیچ دستگاهی بیشتر از نیاز سیستم تهیه نمی شود.

این روش کمترین توان بازیابی خطا یا به عبارت دقیق تر بدون مکانیزم بازیابی خطا است.

مفهوم دیگری هم در این ساختار ها وجود دارد و آن هم نزدیک خط یا Near Line می باشد. این ساختار دقیقا نه روی خط (OnLine)و نه خارج خط (Offline) می باشد نمونه ای از این ساختار پشتیبان گیری بر روی نوار مغناطیسی است. این ساختار در صورت وجود داشتن در شبکه معمولا در ساختار ملایم و سرد برای بازیابی خطا ها کاربرد خواهد داشت.

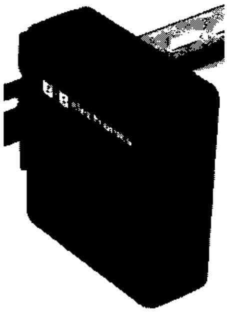
مدیریت انرژی الکتریکی :

یکی از مهمترین بخش های هر برنامه مقاومت در برابر بروز خطا مدیریت انرژی است. رساندن انرژی به سرور ها و دیگر اجزای شبکه اولین اصل در برقراری و پایداری هر شبکه است.هرگونه انحرافی در میزان استاندارد جریان می تواند شبکه و اجزای آن را تحدید و یا دچار اختلال نموده و یا باعث صدمه دیدن تجهیزات شود.

خوشبختانه امروز تجهیزات زیادی وجود دارد که می تواند محافظت از تجهیزات حساس را به آنها سپرد.برخی از آنها عبارتند از :

- محافظ افزایش جریان (Surge Protector)
- منبع انرژی الکتریکی آماده به کار (Standby Power Supply)

❖ منبع بدون وقفه انرژی الکتریکی (Uninterruptable Power Supply)



محافظ افزایش جریان :

این دستگاه از ورود انرژی الکتریکی بالاتر از حد مجاز تعریف شده به تجهیزات که به آن متصل هستند جلوگیری می نماید. این دستگاه هرگونه افزایش ولتاژ الکتریکی را تشخیص داده آن را در حد مجاز تقلیل می دهد و سپس به دستگاه می رساند.یکی از معایب این دستگاه این است که تنها جلوی افزایش بسیار زیاد جریان را می گیرد و افزایش جزیی در جریان از این دستگاه عبور می نماید.

سیستم محافظ با پشتیبانی باتری :

این ساختار سیستم ها را در مقابل قطع جریان الکتریکی محافظت می نماید. در بخش های قبلی در مورد انواع اختلالات جریان الکتریکی صحبت نمودیم.در هنگام قطع کامل جریان الکتریکی این سیستم با کمک باتری هایی که به آن متصل شده است انرژی لازم برای ادامه کار سیستم ها را فراهم می آورد.البته زمان فعالیت آن محدود بوده و بستگی به توان باتری های سیستم می باشد.

⚠ دستگاه های چاپگر لیزری و کپی را به هیچ عنوان نباید به منبع تغذیه متصل نمود.زیرا این تجهیزات انرژی الکتریکی زیادی را مصرف می نمایند و زمان سرویس دهی منبع تغذیه را بسیار کاهش می دهد.

بطور کلی دو سیستم در این ساختار وجود دارد:

❖ SPS:منبع انرژی آماده به کار
❖ UPS:منبع انرژی بدون وقفه

منبع انرژی آماده به کار :

در این ساختار سیستم ها به دستگاه این منبع متصل می شوند مدار ویژه ای در این دستگاه وجود دارد که وضعیت انرژی ورودی را بررسی می نماید ، در صورت قطع شدن انرژی الکتریکی.منبع انرژی ، انرژی مورد نیاز را برای ادامه کار دستگاه ها فراهم می آورد. بخش دیگری در این دستگاه وجود دارد که جریان تولید شده توسط باتری را که جریان مستقیم (DC)است را به جریان برق که متناوب (AC)است تبدیل می نماید.

یکی از معایب این منابع تغذیه بوجود آمدن وقفه بین تبدیل انرژی از برق به باتری است.زیرا در زمان تبدیل وقفه ای کوتاه بوجود می آید که همین وقفه باعث بروز اختلال در عملکرد سیستم های متصل به آن می شود.از این رو این ساختار برای سیستم های رایانه ای مورد استفاده قرار نمی گیرد.

منبع انرژی بدون وقفه:

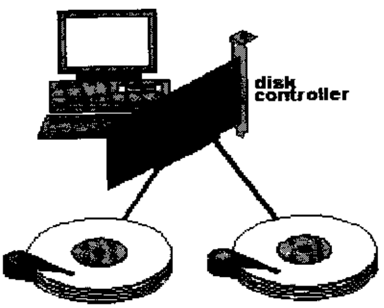
این ساختار نوع دیگری از منابع تغذیه است که امروزه در اکثر سیستم های رایانه ای و شبکه ها مورد استفاده قرار می گیرد.این سیستم همانند ساختار منبع انرژی دارای باتری و مدار تبدیل جریان است اما با در تکنولوژی با هم تفاوت دارند.در این حالت تمامی سیستم های متصل به منبع انرژی ، انرژی مورد نیاز خود را از طریق باتری دریافت می نماید و باتری ها هم همزمان توسط انرژی برق شارژ می شود.در زمانی که انرژی برق قطع شود بدون هیچ وقفه ای سیستم ها می توانند به کار ادامه دهند.

مدیریت داده ها و سیستم های ذخیره سازی:

امروزه دیسک سخت معمولترین ابزار ذخیره سازی در رایانه ها و سرور هاست.برای جلوگیری از بروز مشکل و از بین رفتن داده ها ؛می بایست از تکنولوژی های پیشگیری از بروز خطا استفاده نمود.این تکنولوژی ها عبارتند از :

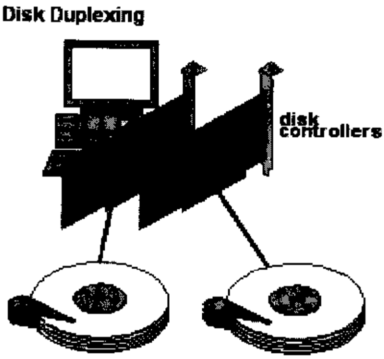
- Mirroring
- Duplexing
- Disk Stripping
- RAID

Mirroring :نسخه برداری انعکاسی



در این روش یک دیسک سخت جدید به رایانه اضافه می شود تا یک رونوشت از تمامی داده های رایانه بر روی آن ذخیره گردد.درصورت بروز خطا در دیسک اصلی از آن می توان برای بازگرداندن داده ها استفاده نمود. لازم به ذکر است برای استفاده از این امکان ظرفیت خالی و قابل دسترس هردو دیسک می بایست یکسان باشد.بطور مثال اگر یک دیسک ۲گیگابایت ودیگری ۳ گیگابایت ظرفیت خالی داشته باشند می توان از ۲ گیگابایت برای این حالت در نظر گرفت.

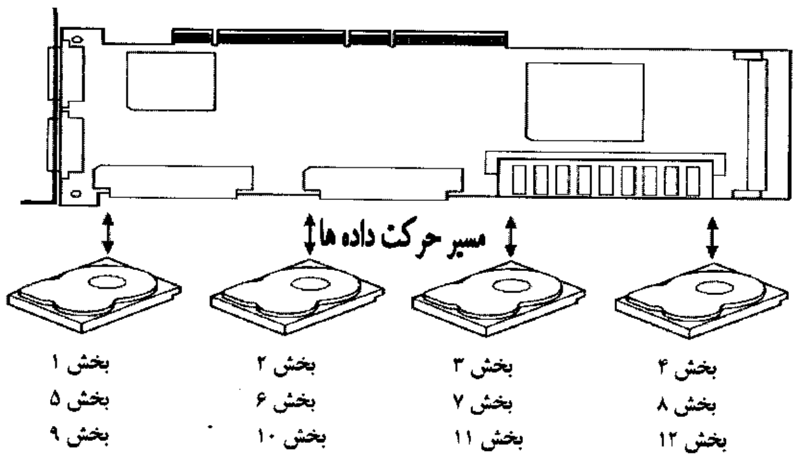
Duplexing:نسخه برداری دوگانه



همانند حالت قبلی ؛ داده ها در یک دیسک دیگر نسخه برداری می شوند. اما تفاوت عمده این دو ساختار در تعداد کارت کنترل دیسک است. در حالت Mirror تنها یک کارت کنترل دیسک وجود دارد که در صورت بروز مشکل در آن هیچکدام از دیسک ها قابل دسترس نخواهند بود. اما در این ساختار هر دیسک یک کارت کنترل کننده مجزا دارد که امکان بروز اختلال در عملکرد سیستم را بسیار کم می نماید.

دیسک Stripping یا دیسک های نواری :

از نگاه کیفیت ؛ نوشتن داده ها بر روی دیسک بسیار کند است.حال اگر شما ۳ دیسک را به حالت نواری تنظیم نمایید اختلاف کیفیت را مشاهده خواهید نمود.این ساختار به شما این امکان را می دهد که داده ها را تقسیم و هرکدام بر روی یک دیسک ذخیره شود. این کار سرعت نوشتن داده ها را بسیار افزایش می دهد.



:(Redundent Array Of Inexpensive Disks) RAID

در این ساختار داده ها بجار قرار گرفتن بر روی یک دیسک با ظرفیت بسیار بالا که بسیار گران است ؛ بر روی مجموعه ای از دیسک هایی باظرفیت کمتر و با قیمت کم قرار می گیرد . شما می توانید از ساختار های متفاوتی برای نوشتن داه ها بر روی دیسک ها استفاده نمایید. انواع مختلف این ساختار به این شرح است:

: RAID0

این روش سریع ترین روش برای نوشتن داده ها بر روی دیسک است. داده ها بدون نسخه برداری بر روی دیسک ها نوشته می شود. این روش از بروز خطا جلوگیری نمی نماید.این روش معادل Disk Stripping می باشد.

: RAID1

این روش معادل Duplexing و Mirroring می باشد.در این روش اگر یکی از دیسک ها دچار اختلال شود دیسک دیگر در سیستم وظایف آن را انجام می دهد زیرا داده ها همزمان بر روی دو دیسک ذخیره شده است.

: RAID2

استفاده از این روش توصیه نمی گردد زیرا داده ها در این روش بر روی تمامی دیسک ها منتقل می شود اما سیستم تشخیص خطا و رفع آن امروزه در تمامی دیسک ها وجود دارد . از این رو دیگر نیازی به وجود این RAID نخواهد بود.

: RAID3

این روش معادل RAID2 می باشد با این تفاوت که در این ساختار داده ها بر اساس بایت منتقل می شوند اما در RAID2 داده ها بر اساس بیت منتقل می شوند.

: RAID4

این روش شبیه RAID2 و RAID3 می باشد.با این تفاوت که داده ها در بلوک های مختلف بر روی دیسک ذخیره می شوند . اما امروزه ساختار متداولی نیست.

: RAID5

در این روش داده ها بر روی ۳ دیسک یا بیشتر نوشته می شوند.در این روش اگر یکی از دیسک ها دچار اشکال شود براحتی می توان آن را تعویض نمود. پس از اتصال دیسک داده ها بر روی آن منتقل می شوند و سیستم مجدد به کار ادامه می دهد.امروزه معمولا این ساختار از ۵ یا بیشتر دیسک تشکیل می شود.

: RAID6

این روش دقیقا معادلRAID5 است با این تفاوت که کارت کنترل آن بسیار گران است از این رو در موارد بسیار خاص استفاده می شود و ساختار معمولی نیست.

> ساختار های دیگری مانند RAID7؛ RAID53:RAID10 هم وجود دارند اما به دلیل اینکه به ندرت از آنها استفاده می شود از آنها نامی برده نشده است.

پشتیبان گیری :

داشتن یک پشتیبان از سیستم می تواند بسیار مهم باشد زیرا درصورت بروز مشکل در سیستم به راحتی می توان سیستم را به حالت عادی باز گرداند.برای داشتن یک پشتیبان مناسب این سوالات بسیار مهم است :

- از چه چیزهایی باید پشتیبان تهیه نمود؟
- چه زمانی باید این کار انجام شود؟
- این پشتیبان باید در کجا ذخیره شود؟
- چه کسی وظیفه تهیه آن را بر عهده دارد؟
- ذخیره سازی بر روی چه رسانه ای انجام می شود؟
- چه نوع ذخیره سازی انجام می شود؟
- از چه نرم افزاری استفاده می شود؟

رسانه ذخیره پشتیبان گیری :

انتخاب یک رسانه مناسب برای ذخیره داه های پشتیبان گرفته شده شاید مهمترین بخش این مبحث باشد.این رسانه می بایست بر اساس حجم داده ها انتخاب گردد. علاوه بر آن باید امنیت آن هم مورد نظر قرار گیرد زیرا در هنگام بروز اشکال در سرور تنها راه بازگشت به حالت اول استفاده از پشتیبان تهیه شده از سرور است.

- امروزه با گسترش تکنولوژی حجم حافظه های قابل حمل و نقل بسیار زیاد شده است که می توان از این حافظه ها برای ذخیره داده های پشتیبان استفاده نمود. این حافظه ها قابل خواندن و نوشتن است یعنی می توان آنها را پاک نمود و داده های جدید تری را جایگزین آنها نمود. این حافظه ها ۲ نوع کوچک تقسیم می شوند. حافظ های کوچک که به آنها حافظه های Flash می گویند در اندازه ای بسیار کوچک امکان ذخیره داده ها در حدود ۳۰ گیگابایت را فراهم می آورد. حافظه های متوسط امکان ذخیره تا ۱ ترابایت داده را فراهم می آورد.
- نوع دیگر رسانه ها درایو های نوری مانند CD,DVD,BlueRay هستند. این رسانه ها قابل خواندن هستند اما یک بار امکان نوشتن بر روی آنها وجود دارد.(البته انواع خاص آنها امکان چندین بار ذخیره سازی

را هم دارند که می توانند داه های گذشته را پاک نمود و داده های جدیدی بر روی آنها ذخیره نمود و یا داده ها را به مرور به آنها اضافه نمود .برخی از این رسانه ها عبارتند ازCD-R، DVD-R)

- نوع دیگری از این رسانه ها نوارهای مغناطیسی هستند.این روش به دلیل آسان و ارزان بودن بسیار مورد توجه قرار می گیرد و در شبکه های بزرگ از این روش استفاده می شود.

ابزار های تهیه پشتیبان :

این ابزار نرم افزار هایی هستند که می توانند از داده ها پشتیبان تهیه نموده و آن را بر روی رسانه مورد نظرتان ذخیره نماید. همچنین می توانند داده ها را قبل از ذخیره کردن فشرده نمایند تا حجم کمتری را اشغال نماید از این رو استفاده از این نرم افزار ها توصیه می شود.

در اکثر سیستم های عامل ،نرم افزار های پشتیبان گیری پیش بینی شده است . البته لازم به ذکر است این نرم افزار ها برای تهیه پشتیبان از سیستم ها بر روی رسانه های خاصی استفاده می شوند. در صورت استفاده از رسانه های خاص می بایست از نرم افزار های مربوط به آنها استفاده نمود.

روشهای تهیه پشتیبان :

پس از انتخاب یک رسانه مناسب برای ذخیره داه های پشتیبان گرفته شده نوبت به انتخاب یکی از روشهای تهیه پشتیبان می رسد.روشهای تهیه پشتیبان بدین شرح است:

- پشتیبان کامل (Full)
- پشتیبان مقطعی (Dffrential)
- پشتیبان افزایشی (Incremental)

پشتیبان کامل :

در این روش از تمام داده ها بصورت کامل پشتیبان تهیه می شود .حجم داده ها در این روش بسیار زیاد می شود. نگهداری داده های پشتیبان گرفته شده نیازمند رسانه هایی با حجم زیادی می باشد.در مواقع اضطراری آخرین نسخه از پشتیبان کامل سیستم برای بازگرداندن سیستم به حالت عادی لازم است زیرا تمامی داده ها در آخرین نسخه پشتیبان وجود دارد.البته تنها داده هایی که در زمان تهیه پشتیبان در سیستم وجود داشته اند قابل

برگشت هستند. یکی از معایب این ساختار همین است زیرا در صورت تهیه پشتیبان در پایان هر روز تمامی داده ها که روز بعد به سیستم اضافه شوند قابل بازگشت نیستند و در صورت بروز اشکال در سیستم از بین خواهد رفت.

پشتیبان مقطعی :

در این ساختار یک پشتیبان کامل در یک بازه زمانی معین مانند یک هفته تهیه می شود. در تمامی روز های هفته بعد تنها از فایل هایی که پس ازتهیه پشتیبان کامل تغییر کرده اند پشتیبان تهیه می شود.پس از پایان هفته مجدد یک پشتیبا ن کامل تهیه می گردد و این چرخه تکرار می شود.

در زمان بروز مشکل در سیستم شما نیاز به استفاده از ۲ پشتیبان را دارید؛ پشتیبان کامل وآخرین پشتیبان مقطعی تهیه شده.

پشتیبان افزایشی :

در این روش هم یک پشتیبان کامل تهیه می گردد.داده هایی که از آنها پشتیبان تهیه شده علامت گزاری می شوند و در زمان تهیه پشتیبان روزانه تنها از داه های جدید پشتیبان تهیه می شود.سپس این داده های جدید هم علامت گزاری می شوند .تفاوت این دو ساختار دقیقا در همین جاست.در پشتیبان مقطعی از داده هایی که نسبت به پشتیبان کامل تغییر کرده بودند پشتیبان گرفته می شد اما در این ساختار تنها از داده هایی که نسبت به آخرین پشتیبان روزانه تغییر کرده اند پشتیبان تهیه می شود. این روش باعث می شود که حجم داده هایی که باید روزانه از آنها پشتیبان تهیه کرد بسیار کاهش پیدا نموده و زمان تهیه پشتیبان را هم کاهش پیدا کند.

شما در هنگام بروز مشکل نیاز به تمامی داده های پشتیبان گرفته شده از ابتدای دوره دارید.

محافظت در مقابل نرم افزار های مخرب و ویروس :

ویروس یک نرم افزار است که پس از ورود به سیستم به سرعت خود را تکثیر و درون سیستم منتشر می نماید و باعث بروز اختلال در عملکرد سیستم می شود. امروزه شاید هزاران نوع ویروس وجود داشته باشد که بخش عمده آنها توسط مراکز تحقیقاتی شرکتهای امنیتی شناسایی شده و راه های مبارزه با آن ها هم مشخص شده است.برای مقابله با آثار مخرب آنها نرم افزارهای ضد ویروس تهیه شده اند که اطلاعات مربوط به ویروس ها را در خود ذخیره نموده و در هنگاه مقابله با آنها از راه های از پیش تعیین شده مانع نفوذ آنها در رایانه ها و یا شبکه می شوند و یا آنها را حذف نموده و مانع انتشار آن در سیستم می شوند .

انواع ویروس ها :

ویروس ها انواع مختلفی دارند که عملکرد هرکدام بر روی سیستم با هم تفاوت دارد.برخی از آنها را در این بخش مشاهده می نمایید :

ویروس های فایلی :

این ویروس ها فایل های اجرایی را مورد حمله قرار می دهند .آنها خود را به فایل اجرایی متصل می کنند و از این طریق بر روی حافظه قرار گرفته و در مدت زمان کوتاهی تمامی فایل های سیستم را آلوده می نمایند.

ویروس های ماکرو :

ماکرو یک اسکریپت است که حاوی فرامینی است که پس از اجرا، نیاز به کمک کاربر ندارد.این ماکرو ها معمولا از طریق فایل هایی که در نگاه اول خطرناک نیستند مانند فایل های Word,Powerpointو ... پنهان می شوند. پس از اجرای فایل آنها هم اجرا می شوند و در کار سیستم اختلال ایجاد می نمایند. البته ماکرو ها همیشه مخرب نیستند و در بسیاری از زمان ها به کمک کاربران می آیند و برخی کارهای تعیین شده را بصورت خودکارانجام می دهند.

ویروس های فضای بوت :

این ویروس ها بر روی فضای ابتدایی دیسک قرار می گیرند.این فضا برای مشخص نمودن سیستم عامل استفاده می شود.پس از قرار گرفتن ویروس در این فضا دیگر امکان بوت شدن و اجرای سیستم عامل نخواهد بود و کاربر پیام عدم وجود سیستم عامل بر روی رایانه را مشاهده می نماید.

به روز رسانی نرم افزار های محافظ :

نکته مهم در مورد نرم افزارهای ضد ویروس به روز بودن آنهاست.زیرا ممکن است ویروسی وارد شبکه شده باشد اما نرم افزار آنتی ویروس مشخصات و نحوه برخورد با آن را نداشته باشد.

شرکت های تهیه کننده نرم افزار های محافظ در برابر ویروس سعی می نمایند که تمامی ویروس ها را بررسی نموده و تنها چند ساعت پس از انتشار آنها راه مقابله با آنها را بدست آورده و آن رابصورت بسته های امنیتی به نرم افزار ها اضافه نمایند.این به روز رسانی می تواند بصورت خودکار از طریق اینترنت یا بصورت دستی توسط کاربر انجام گیرد.

به روز نبودن نرم افزار بسیار خطرناک است اما از نداشتن نرم افزار محافظ بسیار بهتر است.

بررسی سیستم برای آلودگی ویروسی :

بررسی سیستم ها به مراحلی گفته می شود که در آن بخش های مختلف سیستم برای مشخص شدن آلودگی ویروسی مورد بررسی قرار می گیرد. بررسی سیستم های رایانه ای برای آلودگی ویروسی می تواند به ۳ صورت انجام شود.

- بر اساس درخواست کاربر
- در زمان دسترسی و اتصال به سیستم
- بررسی در زمان های اضطراری

بررسی بر اساس درخواست کاربر:

در این حالت شروع بررسی توسط مدیر شبکه یا یکی از کاربران انجام می گیرد.این بررسی می تواند برنامه ریزی شود تا بصورت خودکار در زمانی معین آغاز شود و یا در حالات زیر هم توصیه می گردد:

- پس از نصب هر نرم افزار امنیتی
- پس از بروز رسانی نرم افزار
- زمانی که شما نسبت به سلامت سیستم مشکوک هستید و جهت اطمینان یک بررسی انجام می دهید.

معمولا این بررسی بسته به ظرفیت دیسک ها می تواند زمان بر باشد. توصیه می گردد این بررسی در زمانی خارج از ساعت کاری بوده و یا در زمان شلوغی شبکه نباشد.

بررسی در زمان دسترسی و اتصال به سیستم :

در این حالت بررسی تنها در زمان اتصال به سیستم و یا اجرای فایل ها اجرا می گردد.برخی از حالات که این نوع بررسی اجرا می گردد بدین شرح است :

- وارد کردن یک حافظه Flash
- ذخیره یک فایل از اینترنت
- دریافت یک پست الکترونیکی
- مشاهده یک صفحه اینترنتی

البته باید توجه داشت که اجرای بررسی برروی دیگر برنامه ها تاثیر داشته و سرعت آنها را کاهش می دهد اما در مقایسه با اثرات مخرب ویروس ها می توان چند دقیقه ای این افت سرعت را تحمل نمود.

بررسی اضطراری :

این بررسی زمانی اجرا می شود که ویروس ها به سیستم حمله کرده و کنترل سیستم را به دست گرفته باشند در این حالت با کمک نسخه اضطراری نرم افزار ضد ویروس شما می توانید با حذف ویروس ها مجدد کنترل سیستم را به دست بگیرید.

بازبینی نرم افزار ها :

معمولا اکثر نرم افزار ها دچار ضعف های امنیتی هستند که می توانند امنیت سیستم های رایانه را به خطر بیندازند و یا حریم خصوصی کاربران را به خطر بیندازد که این نقاط ضعف به مرور مشخص می شوند.شرکت های سازنده آنها معمولا بسته هایی افزودنی تولید می نمایند که با اضافه کردن آنها این ضعف ها ترمیم می گردد تا نسخه جدید نرم افزار تهیه شود. توصیه می گردد که همیشه بسته های امنیتی مربوط به نرم افزار ها را دریافت و نصب نمایید تا از بروز خطرات و حملات امنیتی جلوگیری نمایید.

این بسته های امنیتی معمولا در صفحه اینترنتی شرکت سازنده وجود دارد که کاربر می تواند آنها را ذخیره نموده و سپس نصب نماید و یا بروز رسانی خودکار را فعال نموده تا آخرین نسخه ابزار امنیتی بصورت خودکار بر روی رایانه نصب گردد.

جمع بندی:

در این بخش شما:

- **با سیستم های جلوگیری از بروز خطا و باز یابی سیستم پس از خطا بصورت مفصل آشنا شدید.**
- **با سیستم های مدیریت انرژی و ساختار های جلوگیری از بروز خطا در صورت قطع انرژی الکتریکی آشنا شدید .**
- **درخصوص سیستم های ذخیره سازی و ساختار های جلوگیری از بروز خطا در سیستم های ذخیره سازی مطالب مهمی آموختید.**
- **درخصوصنرم افزار های ضد ویروس و اهمیت آنها و اهمیت بروز رسانی به موقع آنها مطالب مهمی آموختید.**

سوالات ارزیابی برای آزمون +Network :

۱ -در کدام ساختار RAID بالاترین درجه امنیت داده ها وجود دارد .

الف) RAID 0
ب) RAID 1
ج) RAID 5
د) RAID 3

۲ -حد اقل تعداد هارد دیسکی که برای ساختار RAID 5 مورد نیاز است.

الف) یک
ب) دو
ج) سه
د) چهار

۳ -کدامیک از این تجهیزات می تواند انرژی الکتریکی بدون وقفه برای سرور ها را فراهم نماید. .

الف) SPS
ب) UPS
ج) USP
د) ESP

۴ – کدام ساختار پشتیبان بالاترین سرعت در انجام و کمترین حجم فایل های ذخیره شده را دارد.

الف) کامل
ب) روزانه
ج) مقطعی
د) افزایشی

۵ -کدام رسانه می تواند بیشترین ظرفیت را برای ذخیره داده ها در اختیار کاربر قرار دهد.

الف) DVD
ب) حافظه USB
ج) دیسک نوری(CD)
د) هارد دیسک

۶ -در هنگام قطع برق کدامیک از تجهیزات نباید به منبع تغذیه جایگزین متصل شود.(تمامی موارد صحیح را مشخص نمایید)

الف) سرور ها

ب) دستگاه کپی

ج) چاپگر لیزری

د) تجهیزات ارتباطی شبکه

۷ -تهیه پشتیبان از داده ها چه امکاناتی را در اختیار شما قرار می دهد . (تمامی موارد صحیح را مشخص نمایید)

الف) مقاومت در برابر نوسان برق

ب) نسخه برداری از داده های حساس شبکه

ج) افزایش سرعت شبکه

د) مقاومت در برابر از دست دادن داده ها

۸ -کدام ساختار بالاترین مقاومت در برابر بروز خطا را دارد.

الف) سایت گرم

ب) سایت ملایم

ج) سایت سرد

د) سیستم تهیه پشتیبان

۹ -مناسبترین زمان برای بروز رسانی نرم افزار های امنیتی کدام گزینه است.

الف) روزانه

ب) هفتگی

ج) سالیانه

د) تنها در زمان بروز حملات به سیستم نیاز به بروز رسانی وجود دارد.

۱۰- ساختار RAID 1 به بیان دیگر .... گفته می شود. (تمامی موارد صحیح را مشخص نمایید)

الف) Duplexing

ب) Copying

ج) Imaging

د) Mirroring

پاسخ به سوالات این بخش

۱ - **ج**

بالاترین ضریب امنیت مربوط به RAID 5 است.

۲ - **ج**

اگرچه در بسیاری مواقع ۴ یا ۵ دیسک سخت استفاده می شود اما حداقل ۳ دیسک لازم است.

۳ - **ب**

تنها UPS بدون وقفه می تواند انرژی را تامین نماید.در ساختار SPS یک وقفه هرچند کوتاه بوجود می آید.

۴ - **ج**

کمترین حجم و زمان تهیه پشتیبان مربوط به ساختار پشتیبان افزایشی است.

۵ - **د**

امروزه با افزایش ظرفیت حافظه USB هنوز هم ظرفیت آنها بسیار کمتر از دیسک سخت است.

۶ - **الف، د**

چاپگر لیزری و دستگاه کپی را هیچگاه نباید به منبع تغذیه متصل نمود زیرا برق زیادی مصرف می نمایند و باعث صدمه دیدن منبع تغذیه می شود.

۷ - **ب ، د**

این کار تنها به محافظت از داده های حساس و نسخه برداری از آنها کمک می کند.

۸ - **الف**

سایت گرم بیشترین و سایت سر کمترین مقاومت در برابر بروز خطا را دارد.

۹ - **الف**

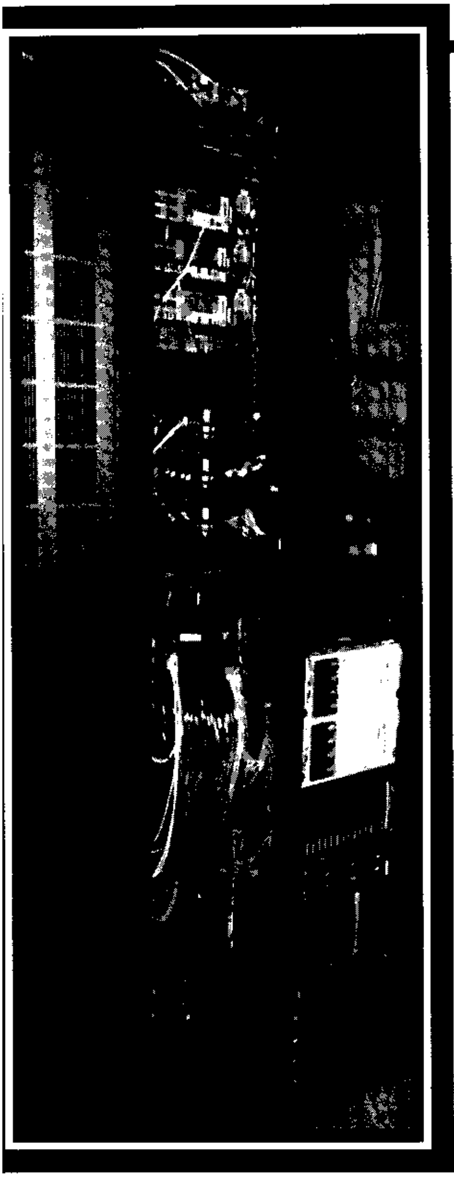
بهترین کار بروز رسانی خودکار است. اما درصورت انجام بروز رسانی توسط کاربر باید هر روز یکبار انجام شود. همیشه باید سیستم بروز باشد.

۱۰ - **الف ، د**

Mirroring و Duplexing در بیان دیگر RAID 1 است.

فصل دهم

عیب یابی شبکه



شما در این فصل با این مفاهیم آشنا خواهید شد:

۱۰-۱ استفاده از چراغ وضعیت در تجهیزات برای شناسایی مشکلات مانند :

- ❖ چراغ برقراری لینک
- ❖ چراغ شناسایی تصادف در شبکه

۱۰-۲ شناسایی خطا های دسترسی به سیستم و نحوه برطرف نمودن آنها نظیر:

- ❖ سرویس اشتراک قرار دادن فایل ها
- ❖ به اشتراک قرار دادن پرینتر
- ❖ اشکالات در شناسایی کاربر
- ❖ مشکلات ارتباط فیزیکی

۱۰- ۳ شناسایی خطاهای رایج در سیستم عامل های مختلف:

- ❖ لینوکس
- ❖ ویندوز
- ❖ سیستم عامل Apple

۱۰- ۴ شناسایی خطاهای رایج در هنگام نصب ، پیکر بندی یا حذف سرویس های متفاوت شبکه

۱۰- ۵ شناسایی محدوده درگیری سیستم ها در صورت بروز خطا ها

فصل دهم- عیب یابی شبکه

مقدمه:

بدون هیچ شک و تردیدی می توان گفت که برای موفقیت در شناسایی خطا ها و رفع آنها تمرین و تمرکز است.این اصل در مورد یادگیری هر هنری هم صادق است. شما باید ابتدا اصول اولیه را بیاموزید و سپس از طریق تمرین ، توانایی خود را تقویت نمایید .

در این بخش سعی شده است مطابق سرفصل های Network + و تجربیات کارشناسان ، نکات مهم و کلیدی در این خصوص را به شما آموزش دهیم اما بخش عمده کار به عهده شماست . شما باید از هر فرصتی برای آموختن استفاده نمایید. در زمان بروز مشکلات تهیه یک یادداشت از نحوه بروز مشکل و سپس طریقه حل شدن آن می تواند به شما بسیار کمک نماید.

البته ذکر این نکته هم ضروری است. همانگونه که به عمد این فصل بخش نهایی کتاب است شما باید مطالب قبلی را آموخته باشید تا این فصل را آغاز نمایید زیرا بخش عمده ای از مطالب این بخش در مباحث قبلی ارایه شده و در اینجا تنها به مواردی از آنها اشاره می نماییم و این بحث در واقع جمع بندی مطالب کتاب است.

محدود کردن دامنه مشکلات:

شاید در مرحله اول شناسایی و رفع اشکال در شبکه کمی دلهره آور باشد. اما اگر دانش کافی داشته باشید این کار می تواند بسیار آسان باشد. ابتدا می بایست دامنه مشکل را کوچکتر کنید.این کار را می توانید با پاسخ به چند سوال بسیار ساده انجام دهید.

- آیا شما به موارد ساده و پیش پا افتاده دقت کرده اید ؟
- مشکل شما سخت افزاری است یا نرم افزاری ؟
- آیا مشکل مربوط به سرور است یا ایستگاه کاری ؟
- آیا فکر می کنید که اشکال مربوط به کابل ارتباطی است ؟

آیا شما به موارد ساده و پیش پا افتاده دقت کرده اید؟

بسیاری از تماس هایی که با شما به عنوان مدیر شبکه برقرار می شود در مورد موارد بسیار ساده است. این موارد را نمی توان دسته بندی نمود زیرا موارد ساده همه جا یکسان نبوده بستگی مستقیم به توانایی و دانش کاربر دارد زیرا ممکن است مشکلی برای یک کاربر بسیار پیچیده و برای کاربر دیگری آسان و قابل حل باشد.اما مواردی وجود دارد که تقریبا همه گیر بوده و بخش زیادی از این مشکلات را در بر می گیرد.معمولا بعد از رفع این

مشکلات کاربر لبخندی می زند که نشان از آسان بودن راه حل دارد و برای زمانی که به آن اختصاص داده بود تاسف می خورد. می توان این موارد را به این گروه های کلی تقسیم نمود:

- مشکلات در ورود به سیستم و مجوز های دسترسی
- عدم دقت به چراغ برقرای لینک
- کلید برق سیستم
- مشکلات سرویس دهنده

مشکلات در ورود به سیستم و مجوز های دسترسی

برای ورود به شبکه و استفاده از منابع آن باید مراحل ورود را بصورت صحیح طی نمود در غیر اینصورت از دسترسی شما به منابع شبکه جلوگیری می شود.

در ابتدا باید کاربر کد کاربری و کلمه عبور را وارد نماید.اشکال زمانی بوجود می آید که کاربر این اطلاعات را به درستی وارد نکرده باشد.ممکن است کلمه عبور را به خاطر نیاورد،کلمه عبور نسبت حروف کوچک یا بزرگ حساس باشد و آنها را به اشتباه وارد نموده باشد، کلمه عبور به زبانی غیر از زبان فعلی تعریف شده باشد و کاربر آن را با زبان دیگری وارد نماید و یا ارتباط شبکه قطع بوده و امکان بررسی آن وجود دارد.در این صورت کاربر نمی تواند به شبکه وارد شود.

مشکل اصلی نبود دقت از سوی کاربر است که به راحتی قابل رفع هستند.

عدم دقت به چراغ برقرای لینک

شاید بدون هیچ تردیدی بتوان گفت بسیاری از افراد بدون دیدن چراغ وضعیت کارت شبکه مشکل شبکه را به گردن مدیر شبکه می اندازند. یکی از وظایف مدیر شبکه بازگو کردن مشکلات معمول برای کاربران و آموزش نحوه برخورد با این مشکلات است. همانگونه که قبلا هم ذکر کردیم این مشکلات می تواند براحتی توسط کاربر رفع شده و مشکلات شما با شبکه و کاربران را بسیار کم نماید.

کلید روشن نمودن دستگاه

تمامی اجزای شبکه و رایانه برای فعالیت نیاز دارند که به یک منبع تغذیه متصل باشند. شاید برای هر مدیر شبکه ای پیش آمده باشد که کاربر اعلام می نماید که رایانه روشن است اما من هیچ تصویری بر روی نمایشگر نمی بینم اولین نکته که به نظر شما می رسد این است که آیا نمایشگر روشن است؟پس از شنیدن صدای شما کاربر بعد از مکثی چند ثانیه ای پاسخ می دهد ممنون از راهنمایی شما.

مشکلات مربوط به برق می تواند بسیار پیچیده هم باشد. مانند ضعف جریان که در مورد آن در فصل های گذشته بصورت تفصیلی سخن گفتیم.اما برخی مشکلات دیگر ممکن است از معیوب بودن کابل یا کلید برق باشد که به راحتی قابل تشخیص نیست.

مشکلات سرویس دهنده

در بسیاری از موارد دلیل اختلال در سرویس ها مشکلات در سمت سرویس دهنده است که خواسته یا ناخواسته شبکه و کاربران را درگیر می نماید.در هنگام برخورد با مشکلات یکی از مبانی عیب یابی بررسی درگاه های ورودی و سرویس ها می باشد. به عنوان مثال در صورت بروز اختلال یا افت سرعت در شبکه اینترنت سازمان، شما می بایست مشکل را در ورودی سرویس به شبکه خود بررسی نمایید و سپس به داخل شبکه بیایید. البته این مراحل به مرور برای شما بصورت یک عادت تبدیل خواهد شد تا باکمک ابزار TCP/IP مشکلات را پیگیری و منبع آن را تشخیص دهید.

مشکل شما سخت افزاری است یا نرم افزاری ؟

شاید اصلی ترین هنر یک مدیر شبکه شناخت مشکلات معمول در شبکه است. زیرا تا شناخت درستی از مشکلات انجام نشود هیچگاه نمی توان برای رفع آنها برنامه ریزی و اقدام نمود.مشکلات سخت افزاری معمولا خود را بصورت اختلال در عملکرد یکی از اجزای رایانه یا شبکه معرفی می نمایند.در این حالت دستگاه در حال عادی مشغول کار است و به یک باره یکی از اجزای سخت افزاری دچار اختلال شده و یا به کلی از فعالیت خارج می شود. معمولا اکثر عیوب سخت افزاری بدون اخطار قبلی دچار این وضعیت می شوند تنها در دیسک سخت قبل از به وقوع پیوستن اختلال ، شما پیام های اخطار را مشاهده می نمایید.

معمولا راه حل در این مواقع تعویض قطعه سخت افزاری است زیرا تعمیر این تجهیزات بسیار مشکل است وشاید از توانایی یک مدیر شبکه خارج باشد.البته در برخی موارد تعویض برخی قطعات هم از عهده مدیر شبکه خارج باشد در آن صورت باید آن را برای یک تکنیسین سخت افزار ارسال نماید.

سخت افزار ها برای فعالیت معمولا یک راه انداز نرم افزاری دارند که در واقع رابط سیستم عامل و سخت افزار هستند. در صورت بروز اشکال در این راه انداز، سخت افزار هم نمی تواند به فعالیت خود ادامه دهد. ابتدا می توانید رایانه را مجدد راه اندازی نمایید در صورتیکه مشکل پابرجا بود نرم افزار راه انداز را مجدد نصب نمایید و در پایان به سراغ تعویض سخت افزار بروید. اجرای این مراحل تجربه شما را در برخورد با این مشکلات بالا می برد و به مرور خواهید دانست در چه مواردی نیاز به تعویض مستقیم سخت افزار و در چه مواردی مشکل تنها با نصب مجدد راه انداز حل می شود.

مشکل مربوط به سرور است یا ایستگاه کاری ؟

در مراحل عیب یابی مهم است که شما مشخص نمایید مشکل مربوط به یک کاربر است یا گروهی از کاربران دچار مشکل یکسانی شده اند. اگر مشکل تنها به یک کاربر محدود است می دانید که مراحل عیب یابی برای کاربر باید اجرا شود. اما اگر گروهی از کاربران درگیر هستند شما کار مشکل تری را پیش رو دارید.زیرا ابتدا باید دامنه مشکل را مشخص نمایید تا پس از بررسی محدوده ، سراغ شناسایی مشکلات احتمالی بروید.این مشکلات می تواند از سرور یا سوییچ های ارتباطی یک بخش از شبکه شما باشد. در این صورت باید تمامی احتمالات را بررسی و راه حل را بیابید.

آیا فکر می کنید که اشکال مربوط به کابل ارتباطی است ؟

با کمک برخی تجهیزات خاص که برای بررسی و سنجش کیفیت کابل ارتباطی و نحوه ارتباط وجود دارد، شما می توانید از کیفیت کابل و ارتباط با آن مطمئن شوید. همچنین نحوه اتصال کابل به کارت شبکه یا سوییچ را هم بررسی نمایید. در بسیاری از موارد عدم اتصال صحیح کابل به سوییچ و کارت شبکه می تواند منشا مشکل باشد. مشکل دیگر می تواند اختلال هایی باشد که توسط امواج الکترو مغناطیسی در کابل ایجاد می شود. این امواج توسط کابل های برق تولید می شود. در صورتیکه کابل شبکه نزدیک کابل های برق باشد احتمال ایجاد این اختلال بسیار زیاد شده و در مواقعی ممکن است انتقال داده ها در کابل شبکه را کاملا مختل نماید. یکی دیگر از مشکلات استفاده از کابل یا اتصال نا مناسب است. اگرچه امروزه اکثر سوییچ ها می توانند هم کابل مستقیم و هم کابل کراس را برای اتصال استفاده نمایند اما در صورت عدم پشتیبانی از این امکان در صورت استفاده از کابل کراس برای اتصال رایانه به سوییچ شما برای تبادل داده ها به مشکل بر می خورید ویا اگر استاندارد های مربوط به اتصال کابل ها(T-568A و T-568B) که در مورد آن قبلا مفصل صحبت کرده ایم را رعایت ننمایید می تواند یکی دیگر از مشکلات کابل های ارتباطی باشد.

گام های عیب یابی :

در مدل پیشنهادی در منابع +Network، ۸ گام برای عیب یابی سیستم و یا شبکه تعریف شده که در این بخش آنها را به ترتیب بررسی می نماییم :

۱. شناسایی نشانه ها
۲. مشخص نمودن منطقه درگیر با مشکل
۳. مشخص نمودن تغییرات
۴. مشخص نمودن دلایل احتمالی

5. پیاده سازی راه حل
6. آزمایش نتایج
7. شناسایی تاثیرات راه حل اجرا شده
8. مستند سازی راه حل

به عنوان مثال هنگامی که یکی از کاربران شبکه به شما به عنوان مدیر شبکه مراجعه می نماید شما باید این مراحل را برای شناسایی و رفع مشکل آن کاربر اجرا نمایید. در این بخش ما بیشتر در مورد این مدل صحبت خواهیم نمود.

گام اول : شناسایی نشانه ها

همانگونه که می دانید اگر شما نتوانید مشکل را تشخیص دهید هیچگاه نمی توانید برای حل آن قدم بردارید. این بحث بسیار شبیه مراحل تشخیص و درمان بیماری توسط پزشک است. شما باید با کمک سوال های ساده سوال کلی را تقسیم بندی نمایید تا بتوانید به مشکل نزدیک شوید. مثلا کاربر از عدم اتصال به اینترنت شکایت دارد شما می توانید با طرح این سوالات به راه حل نزدیک شوید.

شما به کدام بخش اینترنت دسترسی ندارید ؟ آیا تنها به یک وب سایت خاص نمی توانید متصل شوید؟آیا شما می توانید از سرویس پست الکترونیکی استفاده نمایید؟ آیا شما نرم افزار مرورگر دیگری هم در اختیار دارید؟ آیا شما می توانید از نرم افزار پیام رسان استفاده نمایید ؟ مشکل همیشگی است یا اولین بار است ؟

و سوالاتی از این دست که می توانید بر اساس تجربه از کاربر بپرسید، بسیار به شما برای عیب یابی و رفع مشکلات کمک می نماید.

گام دوم : مشخص نمودن منطقه درگیر با مشکل

رایانه ها تجهیزاتی بسیار بی ثبات هستند .ممکن است ماه ها بدون هیچ مشکلی فعالیت نمایند اما به یکباره دچار مشکلات عجیبی می شوند و پس ازرفع آن مجدد شاید ماه ها و سال ها به فعالیت ادامه می دهد اما شاید دیگر آن مشکل را تجربه نخواهد نمود.از این رو می توانید منطقه درگیری با یک مشکل یکسان را مشخص نمایید تا بتوانید عامل احتمالی را شناسایی نمایید و شرایط بروز خطا را شبیه سازی نمایید. از کاربران بخواهید همان کاری را که در زمان بروز خطا انجام داده اند را تکرار نمایند. این راحت ترین کار برای این شناسایی مشکل است.

گام سوم : مشخص نمودن تغییرات

در زمان شبیه سازی بروز خطا باید از کاربر بخواهید که مشخص نماید قبل از بروز خطا چه تغییراتی بر روی سیستم انجام داده است.تغییرات می تواند نرم افزاری بوده که شامل نصب یا تغییر تنظیمات نرم افزار ها باشد و یا

سخت افزاری که شامل افزودن یک قطعه سخت افزاری به سیستم باشد. شما می توانید با طرح چند سوال بسیار ساده از تغییرات سیستم مطلع شده و بتوانید تحلیل درستی از مشکل پیدا نموده و راه حل مشکل را بدست آورد.

- آیا قبلا این کار را انجام داده اید؟

ممکن است کاری که کاربر انتظار انجام آن را دارد با ساختار سخت افزاری و نرم افزاری سیستم قابل اجرا نباشد. اگر کاربر قبلا آن را انجام داده است پس به دلیل بروز مشکلی در حال حاضر قادر به انجام آن نیست. در غیر این صورت باید بررسی نمایید که این کار اصولا قابل اجرامی باشد یا خیر .

- اگر قبلا قادر به انجام کار بوده از چه زمانی دیگر نمی تواند؟

در این صورت باید بررسی نمایید که چگونه این اتفاق افتاده است. اگر درحین انجام کاری سیستم دچار اختلال شده و دیگر امکان انجام آن ممکن نبوده است باید به سراغ اتفاقاتی که در زمان اجرا افتاده است برویم اما اگر بین دو زمان اجرا فاصله ای وجود داشته باید موارد بیشتری مانند تغییرات سیستم بین دو زمان اجرا را بررسی نماییم.

- چه مواردی بین دو زمان اجرا تغییر یافته است؟

پاسخ به این سوال می تواند شما را به سمت منابع ومنشا مشکلات راهنمایی نماید.با مشخص نمودن تغییرات سخت افزاری و نرم افزاری می توان به حل مشکل نزدیک تر شد.شما می توانید با این سوالات شروع نمایید که : آیا چیزی به رایانه شما اضافه شده است ؟ آیا شما کاری را بر خلاف روال همیشگی انجام داده اید؟

- آیا شما اخطار یا پیام خطایی مشاهده نمودید؟

همانگونه که قبلا ذکر نمودیم اکثر مشکلات نرم افزاری دارای یک پیام خطا هستند که بر اساس تو ضیحات و شماره آن می توان آن را کاملا مشخص نمود.فقط کافی است شماره خطا یا توضیحات آن را از کاربر سوال نمایید.

- آیا کاربران دیگری هم این مشکل را تجر به نموده اند؟

یکی از راه حل های مربوط به عیب یابی ، شبیه سازی خطا بر روی سیستم های دیگر است. اگر شما بتوانید مشکل را دقیقا بر روی سیستم های دیگر هم پیاده نمایید مشخص کننده عام بودن خطاست. اما اگر فقط بر روی یک سیستم خاص قابل اجراست می توان مطمئن بود که مشکل تنها بر روی سیستم خاصی است. برخی مشکلات بسیار خاص هستند که تنها مربوط به سخت افزار یا نسخه خاصی از سیستم عامل می شوند.

- آیا همیشه مشکل به یک شکل اتفاق می افتد؟

اگر بتوانیم مشخص نماییم در چه زمان هایی این خطای خاص رخ می دهد بسیار به حل مشکل نزدیک می شویم.به عنوان مثال اگر مشخص شود همزمان با اجرای نرم افزار خاصی خطایی در سیستم عامل بوجود می آید

می توان با بررسی نرم افزار به مشکل پی برد و راه حل آن را تشخیص داد و یا اگر در ساعت خاصی شبکه دچار اختلال می شود می توان با بررسی سرویس مشخص نمود که آیا قانون خاصی برای ساعت مشخص تعریف شده که سیستم را دچار اختلال می نماید.

> این موارد تنها برخی از سوالاتی است که مدیر شبکه می تواند برای رفع مشکل از کاربران بپرسد. سوالات بیشتر را شما باید بر اساس تجربه و دقت در ساختار سیستم خود طراحی نمایید.

گام چهارم : مشخص نمودن دلایل احتمالی

اگر شما مشکل را مشخص نموده و آن را بررسی نموده باشید حال نوبت به مشخص کردن دلایل بروز خطا ها می رسد . این بخش ارتباط مستقیم به آشنایی شما با مبانی شبکه و تجربه عملی دارد. زیرا شما باید با حدس زدن دلایل احتمالی آنها را برطرف نموده تا مشکل رفع گردد. در صورت داشتن دانش و تجربه این مرحله می تواند به راحتی انجام گیرد. در غیر این صورت شاید زمان زیادی را باید صرف آزمون و خطا شود تا دلایل بروز خطا مشخص شود.

گام پنجم : پیاده سازی راه حل

حال که دلایل بروز خطا مشخص شد زمان رفع آنها می رسد. شما باید یک طرح برای رفع مشکلات را اجرا نمایید.این طرح شما باید جامع بوده و مشکلات مشخص شده را در بر بگیرد، در کمترین زمان قابل اجرا باشد؛ بتوان آن را با امکانات موجود انجام داد و کمترین اختلال را بر روی سیستم ، شبکه و کاربران ایجاد نماید. در صورت داشتن این شرایط می توان آن را یک راه حل بهینه و مناسب برای سیستم دانست.

گام ششم : آزمایش نتایج

در این مرحله شما راه حل خود را اجرا نموده و تغییرات مورد نظر را بر روی سیستم انجام داده اید. حال نوبت به بررسی شرایط می رسد که آیا مشکل کاربر حل شده است یا خیر. مثلا کاربر مشکل در ورود به سیستم داشته است شما بررسی نموده و مشخص کرده اید که کلمه عبور کاربر غیر فعال شده است. پس از فعال سازی شما از کاربر می خواهید که برای ورود مجدد سعی نماید. اگر کاربر به سیستم وارد شد نشان می دهد که تمامی مراحل قبلی به درستی اجرا شده و مشکل کاربر حل شده است و اگر مشکل پا برجا بود نشان می دهد شما در یکی از مراحل قبلی دچار خطا شده اید و باید تمامی مراحل را از ابتدا کنترل نموده و اگر نیاز است مجدد اجرا نمایید .

گام هفتم : شناسایی تاثیرات راه حل اجرا شده

شما ممکن است با راه حل خود مشکل یک کاربر را حل نموده باشید اما همیشه به خاطر داشته باشید که شما مدیر یک شبکه هستید نه یک کاربر. شاید راه حل شما مشکل کاربر را حل کرده باشد اما برخی مشکلات در شبکه برای کاربران دیگر ایجاد نموده باشد. از این رو همیشه باید در نقشه و اجرای راه حل تاثیرات دیگر بر روی سیستم و یا شبکه را هم پیش بینی نمایید و تنها یک بعدی به حل مشکل یک کاربر و یا بخشی از کاربران فکر نکنید.

گام هشتم : مستند سازی راه حل

اگر راه حل شما جواب مثبت داشت و تاثیر منفی بر روی دیگر اجزای شبکه نداشت نوبت به مستند سازی تمامی گام های بالا می رسد. شما می توانید تمامی موارد را مستند نموده و ذخیره نمایید تا در صورت بروز مشکل مشابه زمان زیادی را صرف تشخیص و رفع آن ننموده و تنها راه حل را اجرا نمایید. تمامی این مراحل برای سرعت بخشیدن و بهینه سازی زمان شما در شبکه است بطوریکه شما می توانید زمانی را که برای شناسایی مجدد یک مشکل تکراری صرف می نمایید، صرف موارد با اهمیت تر نمایید و از زمان خود بهره بهتری ببرید.

منابع مورد استفاده در عیب یابی :

در طول مراحل عیب یابی و رفع اشکالات شبکه ؛سرور ها و ایستگاه های کاری شما به منابع بسیاری دسترسی دارید که شما را می توانند در روند عیب یابی و رفع اشکال یاری نمایند.در این بخش سعی ما بر این است که برخی از این منابع را بررسی نماییم.

فایل ثبت وقایع سیستم (Log) :

همانگونه که در فصل های گذشته اشاره شد فایل های ثبت وقایع آرشیوی از اتفاقات رخ داده شده در رایانه یا سیستم است و با کمک آن می توان روند سلامتی سیستم در بازه زمانی مشخصی را بررسی نمود. در مورد انواع این فایل ها در گذشته صحبت نمودیم در این بخش هم به دلیل دسته بندی منابع تنها به ذکر نام بسنده می نماییم.

منابع ارایه شده توسط تولید کننده :

تقریبا در تمامی محصولات دیسک فشرده ای حاوی توضیحات و دستور العمل اجرایی وجود دارد که اولین و در دسترس ترین منبع در زمان عیب یابی و رفع اشکال است.شاید یکی از مشکلات که بسیاری از آن شکایت می نمایند عدم وجود منابع به زبان فارسی است که در بسیاری از محصولات شبکه این مشکل وجود دارد.که تنها چاره تقویت زبان انگلیسی است زیرا ۹۹ در صد منابع به این زبان هستند.

پشتیبانی سازنده :

معمولا شرکت های سازنده سخت افزار و نرم افزار زمانی را برای پشتیبانی از محصولات خود معین می نمایند. این پشتیبانی می تواند بصورت حضوری ،تلفنی و یا از طریق پست الکترونیکی باشد.همانگونه که از نام آنها مشخص است سطح هر کدام کاملا مشخص است.بالاترین سطح پشتیبانی مربوط به پشتیبانی حضوری است.در این حالت کارشناسان شرکت به محل مشتری مراجعه نموده و مشکل بوجود آمده را برطرف می نماید.

پشتیبانی از طریق تلفن نیز دارای مزایا و معایبی است. یکی از مزایای آن می تواند بسیار سریع انجام شود و اما عیب آن هم بسیار به این سرعت بستگی دارد . به دلیل همه گیر بودن و محدودیت منابع ممکن است شما برای برقراری ارتباط با کارشناسان زمانی نسبتا طولانی را در پای تلفن منتظر باشید.

اما در مورد پست الکترونیکی بیشترین زمان را برای مطرح نمودن و رفع آن خواهد داشت. زیرا تنها می توان مشکل را مطرح نمود و پاسخ را دریافت نمود و هیچ بحث تعاملی صورت نمی گیرد و در اکثر موارد کمکی به رفع اشکالات نمی نماید.

وب سایت شرکت سازنده :

همانگونه که ذکر شد منابعی که به همراه سخت افزار ها و یا نرم افزار ها ارایه می شوند می تواند بسیار مفید باشد. اما در اکثر اوقات در این منابع نکات ابتدایی و در سطح عمومی ذکر شده است و شاید هم کمی قدیمی باشند . در این صورت می توان اطلاعات جامع تر و به روز را از طریق وب سایت شرکت سازنده مطالعه نمود و یا در تالار های گفتمان محصولات شرکت نمود و از تجربیات کاربران دیگر درمواقع بروز مشکل استفاده نمود. همچنین می توان از امکانات پشتیبانی که بر روی وب سایت می باشد استفاده نموده و سوالات را با کارشناسان شرکت سازنده مطرح نموده و جواب های کارشناسان را دریافت نمایید.

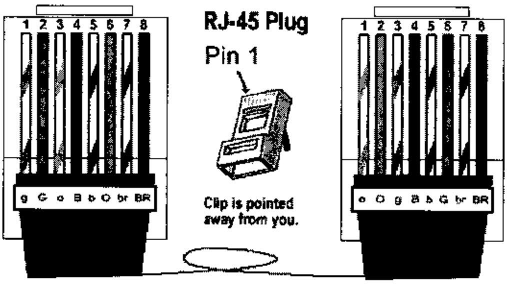
ابزار عیب یابی فیزیکی شبکه :

علاوه بر بسیاری از تجهیزات پیشرفته شناسایی و رفع مشکل که توسط شرکت های مختلف تولید شده اند برخی ابزار های ساده را هم شما می توانید برای عیب یابی شبکه بکار گیرید .در این بخش ۴ ابزار عیب یابی را بررسی می نماییم و آزمون +Network هم شما را در مورد این ابزار آزمایش می نماید. این ابزار عبارتند از :

- کابل Cross-Over
- ابزار سنجش سخت افزاری یا Loopback
- منتشر کننده آهنگ یا Tone Generator
- جستجو گر آهنگ یا Tone Locator

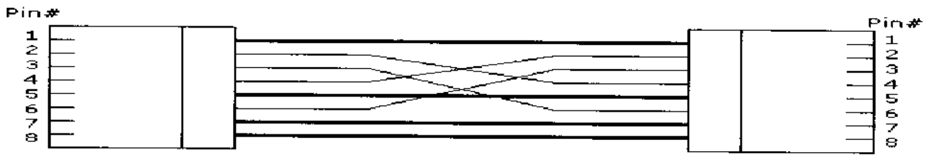
کابل Cross-Over :

این کابل بطور معمول برای اتصال دو هاب به هم مورد استفاده قرار می گرفت اما می توان برای ارتباط مستقیم بین دو سیستم هم از این کابل استفاده نمود.در این کابل یک سر کابل از استاندارد Aو سمت دیگر کابل از استاندارد Bاستفاده می شود.



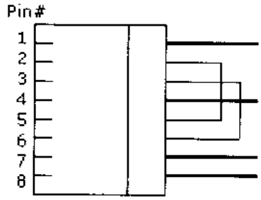
ترتیب رنگ های استفاده شده در دو سر هر کابل به این ترتیب هستند :

۱. سفیدسبز- سبز- سفید نارنجی-آبی - سفید آبی- نارنجی - سفید قهوه ای- قهوه ای
۲. سفید نارنجی- نارنجی- سفیدسبز-آبی- سفید آبی- سبز- سفید قهوه ای- قهوه ای



معمولا همه کارشناسان یک کابل کراس در جعبه ابزار خود و در کیف رایانه همراه خود دارند که از آن برای عیب یابی و رفع اشکالات شبکه و اتصال دو سیستم به هم استفاده می نمایند.

ابزار سنجش سخت افزاری یا Loopback :



این ابزار در واقع یک اتصال ویژه برای کابل های شبکه می باشد.در ابزار که توسط اتصال Rj-45 تهیه می شود مراحل ارسال و رسیدن داده به مقصد در واقع شبیه سازی می شود. یعنی دقیقا گیرنده و فرستنده در یک اتصال قرار دارند.

با کمک این ابزار شما می توانید بررسی نمایید که آیا کارت شبکه توانایی ارسال و دریافت صحیح داده ها را دارد یا خیر. بدون این ابزار بررسی شما برروی توانایی کارت شبکه نمی تواند به راحتی و دقت انجام پذیرد.

منتشر کننده امواج (Tone Generator) و جستجو گر امواج (Tone Locator) :

ترکیبی از منتشر کننده و جستجوگر یک آهنگ بیشتر در کابل های تلفن مورد استفاده قرار می گیرد. از آنجا که معمولا کابل های تلفن دارای زوج سیم های فراوانی در یک کابل هستند مشخص کردن هرکدام از آنها کاری بسیار مشکل و پیچیده است. با کمک این ابزار می توانیم سیم ها را به راحتی مشخص نماییم.

> ⚠ این ابزار را نباید با ابزار ویژه ای که برای سنجش کیفیت و مشخص نمودن زوج سیم خاصی استفاده می شود به اشتباه بگیریم.این ابزار تنها نشان می دهد که زوج سیمی که مد نظر ما می باشد کدام است و همین.



منتشر کننده امواج یک دستگاه الکتریکی کوچکی است که زمانی به سیم متصل شود امواج الکتریکی را درون سیم می فرستد و این امواج در طول سیم در حال حرکت هستند. با کمک جستجوگر امواج می توان مشخص نمود که کدام سیم دارای امواج بوده و از این طریق سیم مورد نظر را مشخص نماییم.

> ⚠ باید دقت نمود که این ابزار را به کابل آزاد متصل نمود.زیرا کابلی که به کارت شبکه یا سوییچ متصل است ممکن است درصورت ورود جریان الکتریکی که توسط منتشر کننده امواج تولید و ارسال می شود دچار صدمه شود.

ابزار عیب یابی نرم افزار ها :

در کنار ابزار سخت افزاری عیب یابی شما می توانید از برخی نرم افزار ها استفاده نمایید تا اطلاعات کاملی از وضعیت سیستم و سلامت آن بدست آورید. این نرم افزار ها به دو گروه زیر تقسیم می شوند :

- نرم افزار تحلیل کننده پروتکل ها
- ابزارهای نظارت بر عملکرد سیستم

نرم افزار تحلیل کننده پروتکل ها :

هر نرم افزاری که بتواند داده های دریافتی را تحلیل نماید را می توان تحلیلگر داده نامید. این نرم افزار می تواند داده ها را بر اساس پروتکل های لایه های پایینی مدل OSI بررسی نموده و اشکالات احتمالی آن را مشخص می نماید.به عنوان مثال شما با کمک این نرم افزار ها می توانید به این نتایج برسید :

- منبع ترافیک شبکه خود را می توانید مشخص نمایید.
- چه پروتکلی بیشتر در شبکه مورد استفاده قرار می گیرد.
- مشخص نمایید که کاربران به چه منابع غیر مجازی دسترسی پیدا می نمایند.

برخی از این نرم افزارها مانند Sniffer در سیستم عامل ویندوز و LAN Analyze در سیستم عامل ناول می باشد.

ابزارهای نظارت بر عملکرد سیستم :

علاوه بر تحلیل گر داده بسیاری از سیستم عامل ها ابزاری برای نظارت بر نحوه عملکرد سیستم دارند که می تواند اطلاعاتی را برای مدیر شبکه به نمایش قرار دهد.برخی از این اطلاعات عبارتند از: حجم داده های ارسالی ،حجم داده های دریافتی،و تعداد بسته های ارسال شده و دریافت شده .

در ویندوز این ابزار Performance Monitor می باشد که در زمان بروز خطا بسیار می تواند به مدیر شبکه برای شناسایی و رفع آن کمک نماید.

نکات کلیدی در عیب یابی :

حال که موارد ابتدایی در مورد عیب یابی شبکه را بررسی نمودیم در این بخش برخی نکات کلیدی را برای کمک به عیب یابی دقیق تر شبکه ذکر می نماییم.با کمک این نکات شما برای مقابله با مشکلات شبکه مجهز تر شده و امکان موفقیت در عیب یابی را افزایش می دهید.

از بررسی موارد ساده و پیش پا افتاده چشم پوشی نکنید.

اگر به یاد داشته باشید اولین مطلبی که در این فصل به آن پرداختیم دقت به مسایل ساده و پیش پا افتاده بود.در برخی موارد مشکلات به دلایل بسیار ساده بوجود می آیند مانند اشکال در پورت و یا مشکل در سرویس دهنده که اگر به آنها دقت نشود ممکن است زمانی چندین ساعته صرف عیب یابی شبکه شود و در پایان به این موارد بسیار ساده برسیم.

شاید برای یک مدیر شبکه با تجربه هم پیش آمده باشد که کد کاربری و کلمه عبور را به اشتباه وارد کرده باشد و یا کابل شبکه را به سیستم متصل نکرده باشد و یا از همه ساده تر کلید برق سیستم را روشن نکرده باشد.اگر به موارد پیش پا افتاده دقت نکند شاید زمانی بسیار زیاد را برای موارد بسیار ساده از دست بدهد.

اگر شما زمانی را برای آموزش برخی موارد ابتدایی به کاربران شبکه در نظر بگیرید می تواند مراجعه های بعدی به شما برای عیب یابی و رفع اشکال آنها را کم نماید. پیشنهاد می کنم که بحث آموزش را جدی گرفته و آن را در محل کار خود پیاده نمایید.

مشکلات را اولویت بندی نمایید

یکی از اصولی که شما به عنوان مدیر شبکه باید بیاموزید چگونگی اولویت بندی در اجرای کار ها می باشد. فرض کنید شما ۳ تماس همزمان از ۳ کاربر شبکه دارید، انتخاب کاربر برای رفع مشکل باید با دقت انجام گیرد. اولویت بندی نشان دهنده هوشمندی شماست که اجرای کارها را بر اساس اهمیت انجام دهید.برخی از مواردی که می تواند در اولویت بندی به شما کمک کند عبارتند از :

- مشکلی که تمام شبکه را درگیر کرده است
- مشکلی که بخش وسیعی از شبکه را درگیر کرده است
- مشکلی که بخش کوچکی از شبکه را درگیر کرده است.
- یک ایستگاه کاری کاملا دچار مشکل است و هیچ کاربری نمی تواند از آن استفاده نماید.
- بخشی از یک ایستگاه کاری دچار مشکل است و کاربر خاصی نمی تواند از آن استفاده نماید.
- یک کاربر دچار مشکلی جزیی است که بعضی اوقات اتفاق می افتد.

برخی از مدیران شبکه تمامی تماس ها را بر روی یک تخته یاد داشت می نمایند. سپس آنها را بر اساس این ساختارکه ذکر نمودیم اولویت بندی نموده و سپس اقدام به رفع آنها می نمایند.در شرکت ها و سازمان های بزرگ نرم افزار های خاصی تهیه شده است که این اولویت بندی را بر اساس قواعد آن مجموعه انجام می دهد و به کارشناسان و مدیر شبکه برای رفع آنها اعلام می نماید.

تنظیمات نرم افزاری و سیستم عامل را بررسی نمایید.

برخی از مشکلات شبکه ممکن است جنبه نرم افزاری داشته باشد.به عنوان مثال در صورت اختلال در سرویس DNS کل شبکه دچار اختلال می شود.لازم به یاد آوری است که هنگامی که شما در حال عیب یابی هستید از تنظیمات مربوط به سرویس های شبکه غافل نشوید. برخی از این سرویس ها عبارتند از :

- سرویس DNS
- سرویس WINS
- رجیستری ویندوز

- فایل Autoexec.bat
- فایل Hosts

به دلیل پیچیده بودن تنظیمات این فایل ها و سرویس ها عیب یابی آنها بسیار دشوار است که نیاز به تخصص ؛ تجربه ؛ دانش و تبحر بالای کارشناس شبکه دارد.

از بررسی وضعیت فیزیکی غافل نشوید.

هدانگونه که در فصل ۶ گفتیم شما به عنوان یک طراح شبکه باید محیط فیزیکی قرار گرفتن سرور ها از نظر دما ؛رطوبت و محل استقرار آنها را با توجه به استاندارد ها طراحی و بهینه سازی نمایید.

در هنگام رفع اشکالات فراموش نکنید که حتما شرایط فیزیکی قرار گرفتن تجهیزات و سرور ها را بررسی نمایید. برخی موارد که می بایست مورد بررسی قرار گیرد عبارتند از :

- دمای بیش از حد محیط
- رطوبت بیش از حد محیط
- رطوبت کم (ریسک تخلیه انرژی الکتریکی)
- مشکلات انرژی الکتریکی
- مشکلات مربوط به اتصال های فیزیکی
- تداخل الکتریکی و الکترو مغناطیسی

کابل های ارتباطی را حتما بررسی نموده و از سلامت آنها مطمئن شوید.

معمولا در موارد اندکی کابل ها منشا مشکلات شبکه هستند اما بروز مشکل در کابل غیر ممکن نیست. اگر شما به کابل شبکه مشکوک هستید ابتدا می توانید کابل متصل به هاب یا سوییچ را بررسی نموده سپس کابل متصل به سیستم و در انتها کابل ارتباطی را بررسی نمایید.برای این کار از ابزار تست کابل استفاده نمایید که در مورد انواع آن در فصل های گذشته صحبت نموده ایم. با استفاده از این ابزار می توان بسیاری از مشکلات کابل ها را بررسی نموده و آنها را مشخص می نماید.برخی از این مشکلات عبارتند از :

- تشخیص شکستگی کابل
- اتصال اشتباه
- تداخل امواج
- طول کابل
- اتصال کوتاه در کابل
- مشکلات در اتصال

برخی از ابزار های پیشرفته تر می توانند مشکلات بیشتری را مشخص نموده یا محل دقیق آن را مشخص نماید. به عنوان مثال می توانند محل دقیق شکستگی در کابل را بر مبنای متر یا فوت مشخص نموده و یا کل طول کابل را مشخص نماید.

سیستم را برای آلودگی احتمالی ویروسی بررسی نمایید.

اکثر کارشناسان در هنگام رفع اشکالات توجهی به نرم افزار آنتی ویروس نمی نمایند زیرا این نرم افزار ها خودکار هستند و نیاز به حضور کاربر ندارند البته خودکار بودن این روال مسوولیت نظارت را از دوش مدیر شبکه بر نمی دارد و همیشه باید بر روی این مراحل ،به روز بودن و اشکالات احتمالی اجرای آن نظارت داشته باشد . یکی از اصلی ترین موارد به روز بودن این نرم افزار است تا اثر مثبتی بر روی شبکه داشته باشد.

اگر شما در سیستم مشکلات و عملکرد های عجیب و ناشناخته ای مشاهده می نمایید ابتدا سیستم را برای آلودگی ویروسی بررسی نمایید. در بسیاری از موارد منشا تمامی این مشکلات درگیری سیستم به ویروس است.

در پایان ذکر این نکته ضروری است که این موارد شاید بخشی از مواردی است که هنگام عیب یابی و رفع اشکال مورد استفاده قرار می گیرد. لازم است هر کارشناس شبکه با توجه به اولویت ها و ساختار شبکه خود لیستی را تهیه نماید و در هنگام عیب یابی از آن کمک بگیرد

جمع بندی:

در این بخش شما:

- ❖ با ۸ گام عیب یابی و رفع اشکال آشنا شدید
- ❖ با فاکتور های فیزیکی مانند چراغ وضعیت کارت شبکه و سوییچ که در عیب یابی به شما کمک می کنند آشنا شدید.
- ❖ درخصوص ابزار های سنجش ارتباط درکابل های شبکه های مطالب مهمی آموختید.
- ❖ درخصوص انواع مراحل شناسایی تا رفع اشکال شبکه ها و منابع در دسترس در این راه مطالب مهمی آموختید.

سوالات ارزیابی برای آزمون Network+ :

۱ -بدون کدامیک از این تجهیزات شما نمی توانید بصورت کامل شبکه را عیب یابی نمایید.

الف) تحلیل گر پروتکل ها
ب) کابل شبکه
ج) کابل کراس
د) ابزار سنجش سخت افزاری یا Loopback

۲-فرض کنید یکی از تجهیزات سخت افزاری شما در ساعت ۲ بامداد روز جمعه دچار اختلال می شود .کدامیک از ابزار عیب یابی را می توانید به راحتی استفاده نموده تا مشکل را به سرعت رفع نمایید.(تمامی موارد صحیح را مشخص نمایید)

الف) دیسک فشرده همراه سخت افزار
ب) وب سایت سازنده
ج) پشتیبانی تلفنی
د) تماس با همکاران دیگر برای مشاوره

۳-گروهی از کاربران از کیفیت پایین سرویس دریافتی خود شکایت دارند اولین قدم برای عیب یابی می تواند کدام کار باشد.

الف) بررسی کارت شبکه سیستم ها
ب) بررسی سوییچ ارتباطی
ج) بررسی کابل ارتباطی
د) بررسی وضعیت سرور

۴- کدامیک از چراغ های وضعیت بر روی کارت شبکه می تواند اولین نشانه برای عیب یابی را نمایش می دهد.

الف) چراغ برقراری ارتباط شبکه
ب) چراغ نمایش تصادف در شبکه
ج) سرعت اتصال شبکه (100/10)
د) چراغ فعالیت شبکه

۵-کدامیک از این تجهیزات برای مشخص کردن سیم مورد نظر بکار می رود .(تمامی موارد صحیح را مشخص نمایید)

الف) منتشر کننده امواج

ب) جستجو گر امواج
ج) آنالیز کننده پروتکل
د) کابل کراس

۶- یکی از کاربران به شما اعلام کرده است که نمی تواند با کلمه عبور و کد کاربری خود به سرور متصل شود و همچنین نمی تواند از اینترنت هم استفاده نماید؛اما دیگر کاربران این مشکل را ندارند. به نظر شما مشکل می تواند کدام یک از موارد باشد .(تمامی موارد صحیح را مشخص نمایید)

الف) کابل شبکه
ب) اختلال در سرور
ج) اشتباه در کلمه عبور
د) مشکل در حقوق دسترسی سرور

۷- یکی از کاربران مشکل با کلمه عبور و کد کاربری دارد. پس از چندین بار ورود کلمه عبور موضوع را به شما اطلاع می دهد. پس از بررسی مشخص می شود که کلمه عبوری که به شما اعلام کرده است صحیح است. به نظر شما مشکل کدام یک از مواردزیر است. (تمامی موارد صحیح را مشخص نمایید)

الف)مشکل در حروف کوچک یا بزرگ هنگام ورود.
ب) مشکل در کابل ارتباطی
ج) مشکل در سرور
د) مشکل در زبان سیستم

۸-کدامیک از این موارد هنگام عیب یابی می تواند به شما بیشترین کمک را انجام دهد. (تمامی موارد صحیح را مشخص نمایید)

الف) وب سایت رسمی سازنده
ب) پشتیبانی تلفنی سازنده
ج) فایل ثبت وقایع
د) سایت های اینترنتی متفرقه

۹- کدامیک از این موارد می تواند در عیب یابی نرم افزاری مورد استفاده قرار گیرد. (تمامی موارد صحیح را مشخص نمایید)

الف) جستجو گر امواج
ب) آنالیز کننده پروتکل
ج) منتشر کننده امواج
د) نرم افزار آنتی ویروس

۱۰-کدامیک از این موارد نمی تواند منشا مشکلات در کابل های ارتباطی باشد. (تمامی موارد صحیح را مشخص نمایید)

الف) تنوع شرکت های سازنده کابل در شبکه

ب) طول کابل

ج) اتصال اشتباه دوسر کابل

د) شکستگی کابل

پاسخ به سوالات این بخش

۱ - د

همانگونه که در مطالب این بخش ذکر شد این ابزار مهمترین ابزار عیب یابی شبکه است زیرا می تواند توانایی کارت شبکه برای ارسال و دریافت صحیح داده ها را آزمایش نماید.

۲ - الف ، ب

اولین منابع در دسترس دیسک فشرده سازنده و وب سایت سازنده است. تنها شرکت های بزرگ پشتیبانی ۲۴ ساعته دارند و امکان برقراری تماس با دیگر همکاران هم در ساعات بامداد روز تعطیل وجود ندارد.

۳ - د

با توجه به درگیر شدن گروهی از کاربران اولین احتمال اشکال در سرور است.

۴ - الف

مهمترین مورد در این حالت برقراری ارتباط است. قبل از برقراری ارتباط موارد دیگر اهمیتی ندارد.

۵ - الف ؛ ب

این ابزار یکی برای وارد کردن سیگنال و دیگری برای جستجوی آن سیگنال دارد که همزمان با هم فعالیت می نمایند.

۶ - الف ؛ ج

مشکل مربوط به یک کاربر است و این مشکل در دسترسی به شبکه است و مربوط به سرور نیست.

۷ - الف ؛ ب ؛ د

به این دلیل که این مشکل مربوط به یک کاربر است و دیگران با آن درگیر نیستند مشکل نمی تواند از سرور باشد.

۸ - الف ؛ب ؛ج

مطالب موجود در وب سایت های متفرقه قابل اعتماد نبوده و نمی توان بر آنها تکیه نمود.

۹ - ب ،د

جستجو گر و منتشر کننده امواج در عیب یابی سخت افزاری مورد استفاده قرار می گیرند.

۱۰ -الف

اگر کابل های استفاده شده در شبکه از شرکت های مختلف باشد هیچ مشکلی در شبکه بوجود نمی آورد به شرطی که همه کابل ها استاندارد باشند.

مطالعه این کتاب به چه کسانی توصیه می گردد؟

اگر شما یکی از هزاران علاقمند به شرکت در آزمون + Network هستید و تصمیم به شرکت در آزمون دارید، درنگ نکنید. زیرا این‌کتاب برمبنای سرفصل‌های مصوب شرکت CompTIA تهیه شده است.

آزمون + Network برای سنجش تجربه و دانش فنی افراد تهیه شده است و هر کارشناس با حداقل ۲ سال کار در زمینه شبکه و با مطالعه‌این کتاب می تواند در این آزمون موفق شود.

برای فراگیری :

- توپولوژی های شبکه ، معایب و محاسن هر کدام
- مدل OSI و لایه های آن
- پروتکل های ارتباطی شبکه
- سخت افزارهای شبکه و عملکرد هر کدام
- سیستم‌های عامل شبکه
- پروتکل‌های امنیت شبکه
- شبکه‌های بی سیم و استانداردهای آن
- شناسایی و نحوه رفع خطاهای شبکه
- ابزار سنجش و آزمایش شبکه
- عیب‌یابی شبکه ها

NAGHOOS PUBLICATION

9 789640 453186

برای خرید Online
به آدرس زیر مراجعه کنید
www.naghoospress.ir